Handboek kennisnet

Aansluiting van het schoolnetwerk op kennisnet

Auteur: Energis/nl.tree - Bert Gerding, Ivar Janmaat, Menno Pieters, Don Stikvoort
Datum: 15 juni 2000
Documentnr: 995047-I
Versie: 20000615.01

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Colofon en Voorwoord

Colofon

Het 'Handboek kennisnet' ('Het Handboek') is een uitgave van nl.tree. Het Handboek wordt regelmatig herzien naar aanleiding van vragen van gebruikers van kennisnet, wijzigingen in het netwerk of de introductie van nieuwe diensten.

Redactie

Menno Pieters (Hoofdredacteur), Frank de Winter (Product Manager).

Adres:

nl.tree
t.a.v. Redactie Het Handboek
Postbus 82097
2508 EB Den Haag
tel.: (070) 8900000
fax: (070) 8900099
e-mail: handboek@kennisnet.nl

Medewerkers aan dit document

Het 'Handboek kennisnet' is gebaseerd op documenten van:

- Bert Gerding (Bos Internet Services)
- Ivar Janmaat (nl.tree)
- Menno Pieters (nl.tree)
- Don Stikvoort (nl.tree)

Verdere bijdragen en opmerkingen zijn ontvangen en verwerkt van (in alfabetische volgorde van achternaam):

- André Demper (nl.tree)
- Mark Koek (nl.tree)
- Fennande van der Meulen (nl.tree)
- Gijs Reitsma (nl.tree)
- Jeroen Oldenhof (Systeembeheerder Drenthecollege)
- Harry Spek (ICT-coördinator Calscollege Nieuwegein)
- Andree Toonk (Bos Internet Services)

Voorwoord

In het Handboek kennisnet ('Het Handboek') wordt een aantal veelvoorkomende vragen en de antwoorden daarop uitgewerkt. Deze vragen zijn voortgekomen uit gesprekken met ICT-coördinatoren, gebruikers en het Ministerie van Onderwijs, Cultuur en Wetenschappen. Getracht is om de uitleg in het document zo levendig mogelijk te brengen en zaken zó uit te leggen, dat ook personen met slechts geringe ervaring met computers aan de hand van dit document aan de slag kunnen.

Het Handboek is slechts bedoeld als een informatief document; het bevat geen uitgebreid overzicht van de diensten van kennisnet. De exacte beschrijvingen van de geboden diensten kunt u terugvinden in de productbeschrijvingen. Afbeeldingen dienen slechts als illustratie, de tekst in Het Handboek is hierbij leidend. **Aan dit document kunnen géén rechten worden ontleend!**

Het Handboek wordt beschouwd als een 'levend' document, daar het regelmatig zal worden onderhouden en bijgewerkt. Indien u op- of aanmerkingen of suggesties heeft, kunt u deze doorgeven aan de redactie van Het Handboek via handboek@kennisnet.nl. Nieuwe versies van Het Handboek zullen op elektronische wijze beschikbaar worden gesteld via de website van kennisnet: http://www.kennisnet.nl/, onder 'Servicepunt'.

Met ingang van versie 20000615.01 is het document opgedeeld in een achttal afzonderlijke delen. Dit is gedaan om de onderhoudbaarheid van het document te verbeteren. Ook kunt u zelf beter kiezen welke delen voor u relevant zijn om te verversen.

Datum : 15 juni 2000 Documentnr.: 995047
Versie : 20000615.01

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel I, Opbouw kennisnet

Indeling van dit document

In Hoofdstuk 1 worden enkele basisbegrippen uitgelegd rond Internet en kennisnet. Er worden vragen beantwoord over hoe kennisnet werkt en hoe computers geadresseerd kunnen worden.

In Hoofdstuk 2 wordt getoond hoe het netwerk van kennisnet er op hoofdlijnen uitziet. De structuur van het netwerk wordt nader toegelicht.

Hoofdstuk 3 geeft weer hoe de IP-reeksen voor aangesloten instellingen zijn ingedeeld.

Inhoudsopgave

Hoofdstuk 1. Kennisnet

Dit hoofdstuk geeft een korte beschrijving van kennisnet. Hierin wordt het een en ander verklaard over wat kennisnet is en hoe het in grote lijnen werkt.

1.1 Wat is kennisnet?

Kennisnet is een initiatief van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het is hierbij de bedoeling om een groot landelijk computernetwerk te realiseren, waarop alle lagere en middelbare scholen en diverse andere onderwijs- en educatieve instellingen aangesloten worden om zo de beschikbare kennis te delen.

1.2 Hoe werkt kennisnet?

Kennisnet werkt op basis van de technologie die ook wordt gebruikt op het wereldwijde Internet. Echter, kennisnet is een gesloten netwerk dat via een zogenaamde firewall op een veilige manier toegang biedt tot de op het Internet beschikbare informatie.

1.3 Wat is de meest bondige karakterisering van het Internet?

Een wereldwijde verzameling onderling verbonden computers die met elkaar ‘praten’ op basis van een taal (‘protocol’) die IP heet: het Internet Protocol. Dat ‘praten’ is geen doel op zich, maar alleen bedoeld als drager van informatiestromen: die informatiestromen worden teweeggebracht door de gebruikers van de computers, en de aard ervan hangt dus af van wat de gebruikers aan het doen zijn.

1.4 Hoe zijn die computers onderling verbonden?

Door middel van verbindende 'kabels'. Die kabels kunnen fysieke kabels zijn (telefoonlijnen, koperen kabels, glasvezels, 'de' kabel (het kabeltelevisienetwerk), LAN-kabels als ethernet, enz.) of draadloze 'kabels' (straalverbindingen, satellieten, enz.).

1.5 Dus een PC op een Woerdense school kan op basis van IP rechtstreeks langs een kabel met een PC in Haren 'praten'?

In principe wel, maar dat gaat niet letterlijk 'langs een (lange) kabel': op de verbinding tussen beide computers bevinden zich waarschijnlijk nog een stuk of tien 'routers'. Routers zijn speciale computers die maar één taak hebben: ervoor zorgen dat IP-informatie de goede kant op gaat. U moet zich namelijk voorstellen dat op het Internet (en ook binnen kennisnet) vele kruispunten van verbindingen bestaan. Op die kruispunten staan dus routers, die de weg weten op het netwerk.

1.6 En de kennisnet-schoolrouter (of ‘kabelmodem’) dan, is dat ook zo'n kruispunt?

Inderdaad, de kennisnet-schoolrouter is een volwaardige router. Het is wel een tamelijk eenvoudige router: hij hoeft alleen maar te beslissen of de IP-informatie die hij op het netwerk van de school langs ziet komen, bedoeld is voor de school intern, of voor daarbuiten (kennisnet of de wijde wereld). Als het voor intern is, laat hij de informatie ongemoeid. Als het voor buiten is, stuurt hij de IP-stroom het kennisnet op, waar een stelsel van grotere routers ervoor zorgt dat de informatie op de plaats van bestemming komt - een andere school, een website of waar dan ook.

1.7 Maar hoe kan een router aan IP-informatie zien waar deze naartoe moet?

Dan moet u eerst weten dat de Internettaal IP alle informatiestromen in stukjes knipt en als kleine 'pakketjes' van informatie verstuurt. Die IP-pakketjes zijn maximaal zo'n 1000 tekens groot (een vol A4tje is ongeveer het viervoudige daarvan) en bewegen zich geheel zelfstandig over het netwerk. Dat kan, omdat elk pakketje is voorzien van een 'dest-address' - een adres van bestemming. Vergelijk het maar met de geadresseerde van een brief. De router nu kan dat 'dest-address' lezen - en weet vervolgens waar hij het pakketje naartoe moet sturen. Dat laatste gaat trouwens net zo hiërarchisch als bij de post: in het geval van de brief van Woerden naar Haren is het echt niet zo dat het postkantoor in Woerden ook de weg in Haren moet kennen om de brief daar ter plekke te krijgen. Daar is een gelaagd distributiesysteem voor.

1.8 Dan is er zeker ook zoiets als een afzenderadres?

Inderdaad: het 'source-address', en dat maakt ook deel uit van elk IP-pakketje. Als dat 'source-address' er niet zou zijn, dan zou een pakketje informatie wel op de computer van bestemming kunnen landen - maar die zou nooit iets terug kunnen sturen, waardoor communicatie onmogelijk zou zijn. In tegenstelling tot de situatie bij de post is de aanwezigheid van het 'source-address' in IP-pakketjes verplicht.

1.9 Maar dan moet elke computer toch een eigen adres hebben?

Wis en waarachtig, ja! Om het Internet - en ook kennisnet - te laten functioneren, moet elke computer een uniek adres hebben - anders is hij niet te vinden. Dit geldt net zo voor routers.

1.10 Hoe zien die adressen eruit?

Die zijn van de vorm '`a.b.c.d`', waar a t/m d getallen zijn van 0 tot 255. Een voorbeeld van zo'n adres is `192.87.13.88`. Zo'n adres is dus uniek voor een bepaalde computer, en die computer is er in principe dus ook mee te vinden op het netwerk.

1.11 Dan deelt er zeker iemand die adressen uit?

Inderdaad, maar dat gaat wel met de nodige slimheid. Er is een wereldwijd gedistribueerd systeem van IP-nummeruitreiking, waarbij de laatste schakel voor de gebruikers wordt gevormd door ISP's, Internet Service Providers, zoals kennisnet. Als een instelling IP-nummers voor haar PC's wil, dan krijgt ze van haar ISP meteen een hele reeks IP-nummers. Dat kan een reeks van acht nummers zijn, maar ook van bijv. 64 of 1024 of nog vele malen meer: afhankelijk van de (aantoonbare) behoefte van de instelling.

1.12 En hoe ken ik zo'n IP-nummer aan mijn computer toe?

Dat kan met de hand (statisch) en dat kan automatisch. Als u het met de hand doet, stelt u de IP-netwerkconfiguratie van de PC zelf in, en u vult dan o.a. het toegekende (statische) IP-nummer in. Voortaan is dat het adres van die computer.

Automatisch kan ook. Dan vraagt de PC iedere keer wanneer hij aangezet wordt, om een IP-adres. Dat adres wordt dan onmiddellijk opgestuurd door een zogenaamde DHCP-server, een computer die niets anders doet dan IP-nummers uitreiken (en weer terugnemen wanneer de bediende PC wordt uitgezet). Het zo verkregen adres wordt vervolgens volautomatisch verwerkt in de PC.

In Windows 98 staat standaard het gebruik van DHCP 'aan'. U hoeft dus niets te doen - mits er een DHCP-server actief is. In deel III van het Handboek wordt uitgelegd hoe een PC met Windows 95, 98 of NT kan worden ingesteld voor het gebruik van DHCP of juist om vaste adressen in te stellen.

1.13 Maar als ik 'internet', hoef ik nooit zo'n IP-adres in te tikken, maar altijd een naam als pc33.laurentius.nl - hoe komt dat?

De reden daarvoor is dat er een dienst op het Internet bestaat, die namen verbindt aan nummers. Die dienst heet DNS: Domain Name System. DNS zorgt ervoor - in het voorbeeld van de vraag - dat als u in een toepassing `pc33.laurentius.nl` intikt, dat die naam dan vertaald wordt in het bijbehorende IP-nummer: het IP-nummer van - in dit vereenvoudigde voorbeeld - een computer die `pc33` heet en die bij `laurentius.nl` hoort, wat bijvoorbeeld de Laurentiusschool in Nederland zou kunnen zijn. Vervolgens gebruikt de bewuste toepassing 'onder de motorkap' alleen nog maar het IP-nummer. De naam is alleen bedoeld voor communicatie met de gebruiker.

Het DNS is eigenlijk een wereldwijde 'gedistribueerde database', dat wil zeggen: het bijhouden van de DNS gegevens is altijd gedelegeerd (gedistribueerd) aan de belanghebbende partij of een vertegenwoordiger daarvan. Delegatie houdt in dat er een top van de boom moet zijn: dat zijn de zogenaamde Root Name Servers, die precies weten waar de DNS informatie voor "`.nl`" en andere van dergelijke zogenaamde "top level domains" te vinden is, zoals "`.de`" voor Duitsland, "`.be`" voor België, "`.com`" voor bedrijven internationaal, "`.edu`" voor onderwijsinstellingen in de USA, enz.

De bijzondere positie die de USA met `.edu` (en ook met bijvoorbeeld `.mil` voor Amerikaanse militaire instanties) inneemt, is overigens een erfenis van de Amerikaanse oorsprong van het Internet.

De informatie voor `.nl` wordt vervolgens bijgehouden door een instantie in Nederland (de Stichting Internet Domeinregistratie Nederland) die op haar beurt precies weet waar de DNS-informatie voor de Internetdomeinen `dsm.nl`, `kennisnet.nl`, `minocw.nl`, `philips.nl` en - in ons voorbeeld - `laurentius.nl` te vinden is. Iets dergelijks geldt voor `.de`, `.com`, `.be`, `.edu`, `.mil` enz.: de kennis is daar waar ze thuishoort.

In ons voorbeeld `pc33.laurentius.nl` is de delegatie daarmee klaar: de plek die de DNS-informatie over `laurentius.nl` bevat, weet welk IP-nummer bij `pc33.laurentius.nl` hoort - en de IP-nummers van alle andere PC´s, servers en netwerkapparatuur van de Laurentiusschool. Het kan de Laurentiusschool zelf zijn die deze informatie bijhoudt, of de school kan het aan een dienstverlenend bedrijf hebben gedelegeerd.

De distributie in DNS kan overigens zo diep gaan als nodig is. Eén niveau dieper dan in het Laurentius-voorbeeld is bijvoorbeeld de systeemnaam `dutrun11.rc.tudelft.nl` voor de machine `dutrun11` op het Rekencentrum van de TU Delft in Nederland. In dat voorbeeld delegeert de Root Name Server naar `.nl`, de `.nl`-name server naar de TU Delft (`tud`)-name server, en de TU Delft name server tenslotte naar de name server van het Rekencentrum (`rc`) van de TU Delft, waar de IP-nummers worden bijgehouden van de machines op het Rekencentrum.

1.14 Wat is het verschil tussen publieke en private IP-nummers?

Zoals gezegd bestaat een IP-adres uit vier getallen van 0 tot en met 255. Hiermee kunnen in theorie 256*256*256*256=4.294.967.296 (ruim 4 miljard) adressen worden gevormd. Dit lijkt heel veel (en eigenlijk is het dat ook), maar doordat lang niet alle adressen worden gebruikt en er relatief inefficiënt wordt omgesprongen met adressen op het Internet, is dit aantal toch onvoldoende.

In een bepaald document (ook wel bekend als RFC1597) is voorgesteld om een aantal reeksen IP-adressen te reserveren voor 'interne' netwerken die niet of niet rechtstreeks zijn verbonden met het Internet: 'private internets'. De betreffende IP-adressen zijn ook wel bekend als 'private adressen' of 'private adresruimte' (Engels: 'private address space'). Deze private adresruimte omvat de volgende IP-reeksen:

- 10.0.0.0 t/m 10.255.255.255;
- 172.16.0.0 t/m 172.31.255.255;
- 192.168.0.0 t/m 192.168.255.255.

Belangrijk is op te merken dat de private adressen niet op het Internet gebruikt kunnen worden, terwijl de zogenoemde publieke adressen wel op het Internet gebruikt kunnen worden. Hierdoor is het bij koppeling van een privaat netwerk aan het publieke Internet nodig om de 'private' adressen af te schermen ('maskeren' of onzichtbaar maken). Door dit afschermen is het op het grensvlak tussen publieke en private adressen niet mogelijk om alle internetdiensten door te laten.

Dit laatste is de belangrijkste reden waarom kennisnet publieke IP-adressen gebruikt.

1.15 Meer informatie

Er is buiten dit document een enorme hoeveelheid informatie beschikbaar over de werking van IP-netwerken. In 'de betere boekhandel' zijn veelal dikke boeken te vinden over protocollen en applicaties. Deze documentatie is voor het overgrote deel in het Engels.

Ook op het Internet is veel informatie beschikbaar. Een goed en (voor wie de Engelse taal beheerst) leesbaar document kunt u vinden op de website van 3Com, onder de titel 'Understanding IP Addressing': http://www.3com.com/nsc/501302.html.

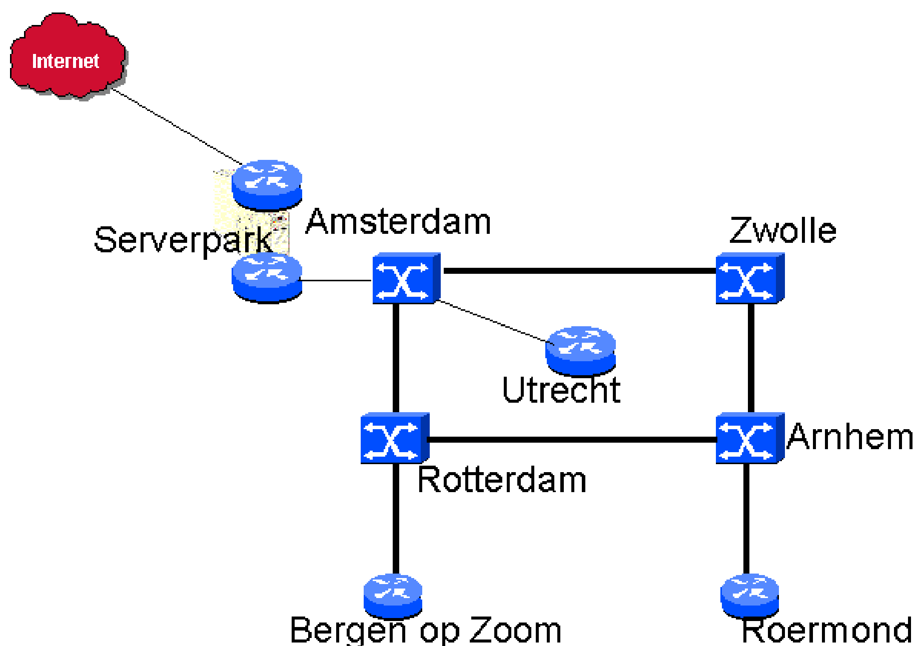
Wie meer technisch is aangelegd en geïnteresseerd is in detailinformatie, kan de zogenoemde RFC- en STD-documenten raadplegen. Dit zijn documenten waarin standaarden worden voorgesteld voor het Internet. Deze documenten zijn onder andere te verkrijgen via FTP op ftp://ftp.ripe.net/rfc/, respectievelijk ftp://ftp.ripe.net/std/.

Hoofdstuk 2. Het netwerk

In dit hoofdstuk wordt uitgelegd hoe het kennisnet eruit ziet. De belangrijkste zaken, zoals de 'backbone' (Nederlands: ruggengraat) en het serverpark, worden uitgewerkt.

2.1 Backbone

Het hoofdonderdeel van het netwerk is de 'backbone'. Deze backbone bestaat uit verbindingen tussen Amsterdam, Rotterdam, Zwolle en Arnhem, en verzorgt de verbinding tussen alle aansluitingen van de netwerken van de partners van het kennisnetproject (regionale kabelmaatschappijen) en het serverpark.



Figuur 1: de 'backbone' van kennisnet met de belangrijkste verbindingen

In Figuur 1 is een schematische afbeelding van de backbone van kennisnet weergegeven. De blauwe vierkante objecten zijn zogenoemde ATM-switches, die onder andere zorgen voor de verdeling van capaciteit van het netwerk naar behoeften. De blauwe ronde objecten zijn hoofdrouters van kennisnet, waarop belangrijke netwerkonderdelen van onder andere de regionale kabelmaatschappijen aankoppelen.

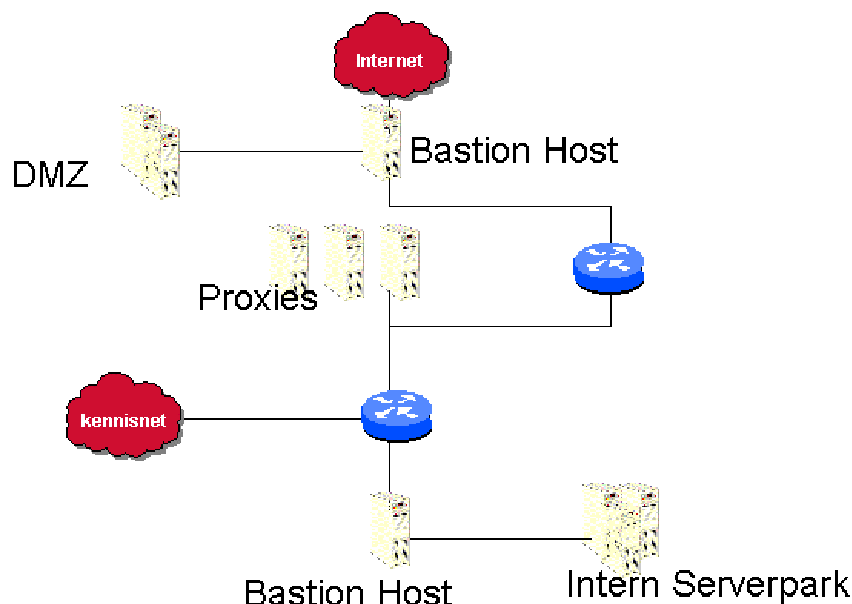
Tussen het serverpark en elk zogenoemd uitkoppelpunt (de plaats waar de kabelmaatschappij haar netwerk koppelt aan de backbone) zijn twee virtuele verbindingen gemaakt. Verkeer vanaf een schoollocatie naar het serverpark kan daardoor via twee verschillende (virtuele) routes over de backbone zijn bestemming bereiken.

2.2 Het serverpark

Het serverpark van kennisnet is de plaats waar alle diensten die kennisnet aan de gebruikers aanbiedt, ondergebracht zijn. Er staan vrij zware (letterlijk en figuurlijk!) computersystemen (servers) die belangrijke taken uitvoeren om kennisnet naar behoren te laten functioneren.

Het serverpark is, hoewel fysiek alles op dezelfde locatie staat, in drie delen op te splitsen:

- het interne serverpark;
- het externe serverpark (DMZ);
- de proxies.



Figuur 2: schematische weergave van het serverpark

Naast de genoemde onderdelen worden bepaalde stukken van het netwerk zijn er 'bastion hosts' aanwezig. Dit zijn systemen die actief netwerkverkeer controleren en bepalen of verkeer al dan niet mag worden doorgelaten. Vaak worden dergelijke systemen als 'firewalls' aangeduid.

2.2.1 Het interne serverpark

Het interne serverpark is de plaats waar de meeste computersystemen ('servers') staan, welke diensten aanbieden aan de gebruikers van kennisnet. Hierbij kunt u denken aan de mail- en newsservers, een interne webserver, de centrale DHCP- en DNS-servers en nog enkele belangrijke systemen.

Deze servers hebben géén rechtstreeks contact met de buitenwereld en zijn niet rechtstreeks van buiten kennisnet te benaderen. Dit is zo gemaakt om kennisnet en de vitale systemen optimaal te kunnen beschermen. Sommige van deze machines hebben echter wel een bepaalde vorm van contact met de buitenwereld nodig (denk bijvoorbeeld aan uitwisseling van e-mailberichten). Dit gaat **altijd** via de servers in het externe serverpark.

2.2.2 Het externe serverpark (DMZ)

In het externe serverpark, ook wel DMZ (DeMilitarized Zone) genoemd, staan de computersystemen die een belangrijk deel van de communicatie met de buitenwereld verzorgen. Zo staan hier de webservers van kennisnet en de DNS-servers die ervoor zorgen dat de systemen van kennisnet (en van de scholen) op het Internet te vinden zijn. Ook staan hier computersystemen die e-mail en news doorsturen van het Internet naar kennisnet en andersom. Deze laatste worden ook wel 'relays' genoemd.

2.2.3 De proxies

Het woord 'proxy' betekent 'gevolmachtigde' of 'vertegenwoordigd'. Ofwel: een proxy is iemand die namens u een handeling verricht. In dit geval het ophalen van gegevens vanaf het Internet of een verbinding maken met een systeem op het Internet. Dit is dus de taak van de proxyservers. Deze machines zijn de enige machines die naar 'buiten' mogen en vormen ook de scheiding tussen de 'binnenkant' en de 'buitenkant' van het netwerk van kennisnet.

Hoofdstuk 3. Indeling van lokale IP-adressen

Dit hoofdstuk geeft informatie over hoe de netwerkadressen van aangesloten instellingen worden ingedeeld.

3.1 Basisbegrippen

Wellicht is het nuttig allereerst de basisbegrippen van IP-reeksen kort uit de doeken te doen. Het netwerkadres is altijd het onderste adres uit een reeks, maar het netwerkadres is *niet* bruikbaar als IP-adres voor een machine. Het hoogste adres uit een reeks, bekend als het zogenaamde 'broadcast address' (omroepadres), is bedoeld om alle aanwezige machines in een netwerkreeks aan te spreken; dit is nuttig voor sommige protocollen. U dient dus altijd twee adressenaf te trekken van het aantal IP-adressen in een reeks, om het aantal bruikbare adressen te verkrijgen.

Voorbeeld. Gegeven een IP-reeks met netwerkadres 10.123.45.0 en 128 adressen. Het 'broadcast address' is dan het hoogste adres uit de reeks: 10.123.45.127. Het eerste bruikbare adres om uit te delen aan een computer is dan 10.123.45.1 en het laatste is dan 10.123.45.126.

De grootte van een reeks IP-adressen wordt meestal aangeduid met een zogenoemd netwerkmasker ('net mask'). Dit ziet eruit als een soort IP-adres, maar geeft in wezen aan hoeveel bits in het adres relevant zijn voor de betreffende reeks IP-adressen. Ieder stukje uit een IP-adres of een netwerkmasker is een getal van 0 tot 255, waardoor ieder stukje binair in exact acht bits kan worden gerepresenteerd.

Door een binaire 'AND'-operatie uit te voeren van het netwerkmasker op een willekeurig adres uit de reeks, wordt het netwerkadres verkregen. De binaire AND-operatie houdt in dat alle bits één voor één met elkaar worden vermenigvuldigd: overal waar in het netwerkmasker een '1' staat, blijft het bit op dezelfde positie in het adres ongewijzigd; waar een '0' staat, wordt het bit op dezelfde positie in het adres ook een '0'.

Met deze AND-operatie definieert u een 'subnet'. Een subnet is een gedeelte van een groter netwerk, bestaande uit een groter aantal IP-adressen

Voorbeeld. In het eerder gegeven voorbeeld is het netwerkmasker 255.255.255.128. De binaire representatie hiervan is `11111111.11111111.11111111.10000000`. Een adres uit de reeks is bijvoorbeeld 10.123.45.67. Dit kan binair gerepresenteerd worden als `00001010.01111011.00101101.01000011`. Door nu de AND-operatie uit te voeren, ontstaat het volgende.

IP-adres	`010.123.045.067`	`00001010.01111011.00101101.01000011`
Net Mask	`255.255.255.128`	`11111111.11111111.11111111.10000000`
Netwerkadres	`010.123.045.000`	`00001010.01111011.00101101.00000000`

Een netwerkmasker wordt ook wel aangegeven met een schuine streep, gevolgd door een getal. Het getal geeft het aantal 'enen' in het netwerkmasker aan (de enen zijn altijd aaneengesloten). Zo kan het hierboven genoemde masker ook worden aangeduid als een '`/25`' (uitgesproken als '*slash vijfentwintig*').

3.2 Indeling IP-adressen

Alle schoolrouters worden (of in bestaande gevallen: zijn) voorzien van filters. Deze filters delen de IP-reeks van uw schoolnetwerk in de volgende stukken:

- de router;
- één gereserveerd adres;
- werkplekken;
- lokale servers die op kennisnet 'zichtbaar' moeten zijn;
- lokale servers die *niet* op kennisnet 'zichtbaar' moeten zijn en overige netwerkapparatuur (hubs, routers, switches).

De indeling van de IP-adressen is voor *alle* kabelmaatschappijen en Energis gestandaardiseerd.

In netwerken met 32 of 64 adressen (netwerkmasker `255.255.255.224` of `255.255.255.192`) wordt 3/4 (min de router, min een gereserveerd adres) van de adressen gebruikt voor werkplekken, 1/8 is bestemd voor servers die zichtbaar moeten zijn op kennisnet, en 1/8 voor afgeschermde servers.

Voor netwerken met 128 of meer adressen wordt 7/8 van de adressen (min de router, min een gereserveerd adres) gebruikt voor werkplekken, 1/16 is bestemd voor servers die zichtbaar moeten zijn op kennisnet, en 1/16 voor afgeschermde servers.

Er volgt nu een aantal voorbeelden van IP-reeksen en netwerkmaskers. **Let op:** dit zijn fictieve adressen.

Voorbeeld (netwerkmasker: `255.255.252.0`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.252.0`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.2.3`, start servers zichtbaar: `212.180.3.128`, servers niet zichtbaar: `212.180.3.192`.

Voorbeeld (netwerkmasker: `255.255.254.0`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.254.0`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.0.3`, start servers zichtbaar: `212.180.1.192`, servers niet zichtbaar: `212.180.1.224`.

Voorbeeld (netwerkmasker: `255.255.255.0`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.255.0`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.0.3`, start servers zichtbaar: `212.180.0.224`, servers niet zichtbaar: `212.180.0.240`.

Voorbeeld (netwerkmasker: `255.255.255.128`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.255.128`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.0.3`, start servers zichtbaar: `212.180.0.112`, servers niet zichtbaar: `212.180.0.120`.

Voorbeeld (netwerkmasker: `255.255.255.192`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.255.192`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.0.3`, start servers zichtbaar: `212.180.0.48`, servers niet zichtbaar: `212.180.0.56`.

Voorbeeld (netwerkmasker: `255.255.255.224`):

Netwerkadres: `212.180.0.0`, netwerkmasker: `255.255.255.224`, router: `212.180.0.1`, gereserveerd adres: `212.180.0.2`, start DHCP: `212.180.0.3`, start servers zichtbaar: `212.180.0.24`, servers niet zichtbaar: `212.180.0.28`.

Rekenhulpmiddel

Op http://enbvlists.kennisnet.nl/techniek/ vindt u een webpagina die u kunt gebruiken om de voor u toepasselijke IP-gegevens te berekenen. U dient hiervoor één IP-adres en het netwerkmasker bij de hand te hebben. Als het goed is, heeft u deze van nl.tree ontvangen bij de aansluiting of, in het geval van voorhoedescholen, bij de IP-migratie [1].

[1] In de proeffase van kennisnet heeft er een omnummeroperatie plaatsgevonden m.b.t. de IP-adressen op kennisnet.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u een e-mail sturen aan 'handboek@kennisnet.nl'.

Index

Figurenlijst

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel II, Fysieke aansluiting

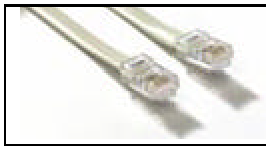
Inhoudsopgave

Hoofdstuk 1. Fysieke aansluiting

Dit hoofdstuk gaat in op vragen over hoe het lokale netwerk van een school fysiek kan worden aangesloten op het kennisnet, ervan uitgaand dat er een aansluiting is opgeleverd door de betreffende kabelmaatschappij, RTB of Energis (ISDN VPoP en huurlijnen).

1.1 Wat wordt er opgeleverd?

Een aansluiting op kennisnet betekent dat u een zogenoemd RJ45-stopcontact krijgt. Hierop kunt u middels een standaard ethernetkabel (categorie 5; zie Figuur 1) een computer of computernetwerk aansluiten. Wat er achter dit stopcontact gebeurt, zou voor de gebruikers transparant moeten zijn, ongeacht de gebruikte soort aansluiting.



Figuur 1: RJ45-bekabeling[1]

De geleverde aansluiting kan een kabelmodem zijn of een router. Indien een los kabelmodem en een losse router zijn geleverd, dient u te koppelen aan de router.

1.2 Hoe sluit ik een enkele computer aan op kennisnet?

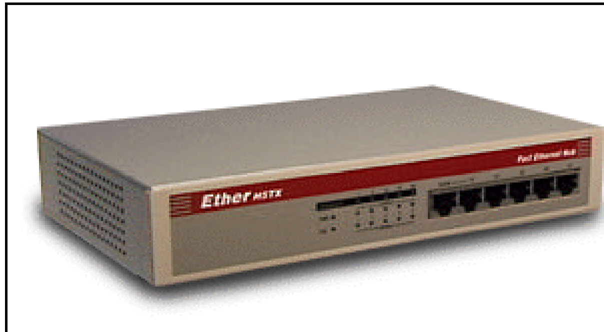
U kunt een enkele computer aansluiten op het RJ45-stopcontact door middel van een zogenoemde kruiskabel. U kunt een dergelijke kabel herkennen door beide stekkertjes naast elkaar te houden. Normaal gesproken zijn deze stekkertjes doorzichtig en in het geval van een kruiskabel zult u zien dat enkele van de gekleurde draadjes van positie verschillen.

Indien u de juiste kabel hebt gebruikt, zal zowel op de kennisnetaansluiting als op de netwerkkaart van de computer een klein lampje gaan branden, indien beide apparaten zijn ingeschakeld. Indien dit niet het geval is, controleer dan of op de PC ondersteuning voor uw netwerkkaart is geïnstalleerd en of u de juiste kabel hebt gebruikt.

1.3 Hoe sluit ik mijn lokale netwerk aan op kennisnet?

Voor het aansluiten van meerdere computers in een netwerk op kennisnet dient u gebruik te maken van één of meer hubs.

[1] [bron afbeelding: http://www.accesscomms.com.au/]



Figuur 2: ethernet-hub[2]

Een hub is een apparaat dat het netwerkverkeer distribueert zonder zich met de inhoud van het verkeer te bemoeien. U kunt eenvoudig meerdere computers koppelen door middel van normale UTP-ethernetkabels (categorie 5).

Veelal heeft een hub een kruispoort of een poort die (door een schakelaar) als gewone en als kruispoort kan functioneren. De kruispoort kunt u gebruiken om de hub middels een kruiskabel aan uw kennisnet-aansluiting te koppelen. Indien u uw aansluiting aan een gewone poort wilt koppelen, dient u een normale ethernetkabel te gebruiken.

U herkent een gewone ethernetkabel door de beide stekkertjes naast elkaar te houden. Het zal u opvallen dat alle gekleurde draadjes op beide stekkertjes in dezelfde volgorde zitten.

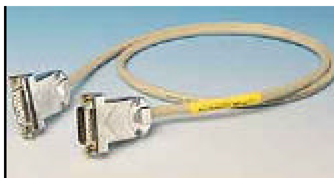
Indien alle kabels correct zijn aangesloten en de betreffende apparaten zijn ingeschakeld, zal op de hub voor iedere aansluiting een klein lampje gaan branden, evenals op de aangesloten apparatuur.

1.4 Mijn lokale netwerk is niet gekoppeld met UTP, maar met BNC/AUI. Wat nu?

Mijn lokale netwerk is niet gekoppeld met UTP (dun kabeltje met een klein stekkertje), maar met BNC (coaxkabels met een ronde bajonetsluiting) of AUI (coaxkabels met een D-vormige stekker). Wat nu?



Figuur 3: BNC[3]



Figuur 4: AUI[4]

Het koppelvlak van de kennisnetaansluiting is inderdaad een ‘female’ UTP-contact. Het coaxsysteem en het UTP-systeem maken echter gebruik van dezelfde ethernettechnologie. Een bestaand coaxnetwerk met het UTP-contact verbinden, is daarom geen probleem: men dient slechts te beschikken over een ‘hub’ waarop zowel coax als UTP kan worden aangesloten. Mogelijk zijn zulke hubs al in het eigen netwerk aanwezig!

Zo niet, dan zijn ze vanaf ongeveer NLG 150 (EUR 68) te koop (4 UTP-poorten en 1 BNC; AUI is iets duurder dan BNC). Let wel op of het eigen coaxnetwerk met AUI (D-vormige stekkers) of BNC (pluggen met bajonetsluiting) werkt, en of de hub in het net kan worden geplaatst. Indien u over een 'fast ethernet'-netwerk beschikt, kunt u het beste een 'dual speed' hub voor 10 of 100 megabit per seconde (Mb/s) aanschaffen. Deze zijn vanaf ongeveer NLG 300 (EUR 136) te koop.

---

[2] [Bron afbeelding: http://www.netlux.com/]

[3] [Bron afbeelding: http://www.net-shop.co.uk/productf/cacoaxef.htm]

[4] [Bron afbeelding: http://www.net-shop.co.uk/productf/cacoaxef.htm]



Figuur 5: T-stukje BNC[5]

Voor dat laatste is bij AUI een vrije ‘transceiver’ nodig, die met een ethernet AUI-kabel met D-stekkers wordt verbonden met de hub; bij BNC volstaat het aanbrengen van een extra BNC T-stukje in de bekabeling, waarbij de poot van de ‘T’ wordt aangesloten op de BNC-ingang van de hub. Let altijd goed op of er ‘male’ of ‘female’ verbindingen worden gebruikt.

Als de hub in het coaxnetwerk is aangesloten, dient alleen nog de hub met een UTP-kabeltje (‘straight’ kabel, geen kruiskabel) te worden verbonden met de kennisnet UTP-poort. Gebruik altijd UTP-bekabeling van categorie 5. Dergelijke bekabeling is toekomstvast. Zorg dat de kabels niet langer zijn dan zo'n tien meter; dat is een veilige bovengrens om storingen in het netwerkverkeer te voorkomen.

Bij afwezigheid van enige kennis van het bovenstaande is het raadzaam een netwerkleverancier of een terzake kundige collega of derde te raadplegen. Het is geen moeilijke materie en er kan weinig fout gaan, maar als de kennis geheel ontbreekt, is de communicatie met een winkelier over wat nodig is erg lastig.

1.5 Het lampje op de hub/switch of mijn netwerkkaart gaat niet branden. Wat nu?

Er kan van alles en nog wat mis zijn. Hier volgen wat mogelijke oorzaken en oplossingen.

- Dit probleem komt nogal eens voor bij het gebruik van 10Mbit ethernetkaarten in combinatie met een 10/100Mbit hub of switch. Probeer eens om een andere hub (10Mbit) tussen de 10/100Mbit hub en de PC te plaatsen; vaak lost dit het probleem op.
- Het probleem kan ook zitten in de bedrading. Wanneer een kabel niet goed is of u, in plaats van een normale kabel, een kruiskabel gebruikt, zal het lampje behorende bij de aansluiting niet gaan branden. Probeer dan een andere netwerkkabel.
- Wanneer een PC de netwerkkaart niet herkent (veelal doordat de besturingssoftware geen ondersteuning biedt voor de kaart), gaat het lampje meestal niet branden. Controleer of u de juiste 'drivers' (stuurprogramma's) hebt geïnstalleerd en/of informeer of er al ondersteuning voor een netwerkkaart is bij uw besturingssysteem.
- Soms heeft een hub een 'uplink-poort'. Deze fungeert als kruispoort, waarmee u verbindingen met andere hubs kunt realiseren. Op deze poort kunt u geen PC aansluiten met een gewone kabel, wel met een kruiskabel. Soms zit er een knopje op om te schakelen tussen een normale poort en een kruispoort; soms is de poort dubbel uitgevoerd. U kunt in het laatste geval slechts één van beide poorten gebruiken, anders zullen geen van beide het doen.

[5] [Bron afbeelding: http://bugs.wpi.edu:8080/EE535/hwk97/hwk5cd97/yqin/sc1.htm]

1.6 Treedt er performanceverlies op wanneer ik de hub rechtstreeks op de kennisnet-router aansluit?

U zult altijd een hub of switch moeten gebruiken om uw netwerk aan de kennisnetrouter te koppelen. Indien het lokale verkeer (dus tussen uw werkstations en servers onderling) geen al te grote belasting op de hub is, zal de hub niet de beperkende factor zijn. Indien u wel veel lokaal verkeer hebt, zou het gebruik van een switch enige verbetering kunnen brengen. Uiteraard is het zinvol om een hub of switch te gebruiken die 100Mb/s of gemengd 10Mb/s en 100Mb/s aankan.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u een e-mail sturen aan 'handboek@kennisnet.nl'.

Index

Figurenlijst

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel III, Software

Indeling van dit document

Hoofdstuk 1 gaat in op de softwareconfiguratie voor gebruikers: hoe kunt u Windows en MacOS zo instellen, dat deze op kennisnet correct werken. Daarnaast wordt ingegaan op de instellingen die nodig zijn voor diverse toepassingen: web, FTP, e-mail, IRC, telnet.

In Hoofdstuk 2 wordt het een en ander uitgelegd over netwerkadressen: welke worden via DHCP uitgedeeld en welke kunt u vrij indelen. Ook wordt een aantal belangrijke adressen opgesomd.

Hoofdstuk 3 bevat een overzicht van veelvoorkomende en belangrijke (fout)meldingen die kunnen voorkomen bij het gebruik van kennisnet en het Internet. Er wordt hier ingegaan op meldingen van web, FTP en e-mail.

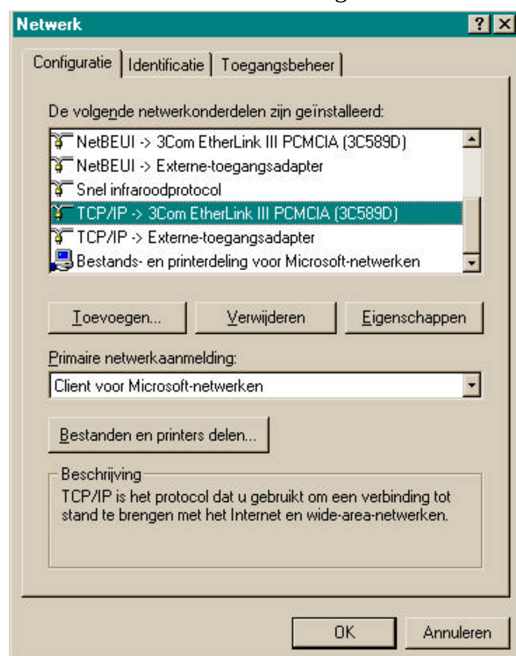
Inhoudsopgave

Hoofdstuk 1. Software-instellingen

Dit hoofdstuk geeft antwoord op vragen hoe software kan worden ingesteld om gebruik te maken van kennisnet.

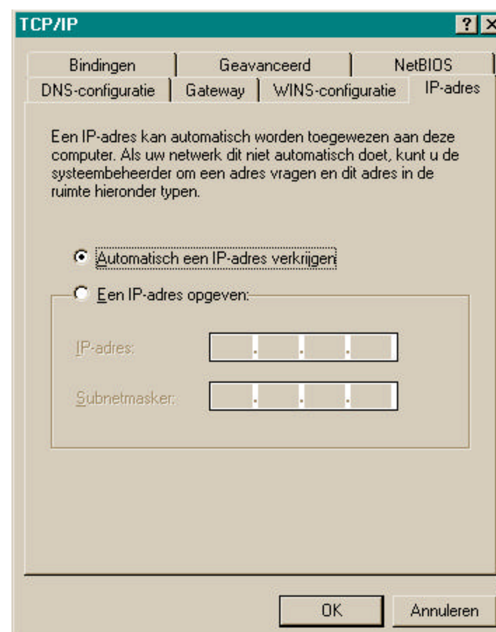
1.1 Hoe stel ik Windows 95/98/NT in?

Kennisnet gaat uit van dynamische toekenning van IP-nummers aan werkstations op scholen d.m.v. het zogenoemde DHCP-protocol. Dat houdt in, dat op de werkstations in het 'configuratiescherm' onder 'netwerk' alleen hoeft te worden aangegeven dat IP-nummers automatisch worden verkregen. Verder moet daar dan **niets** worden ingevuld.



Figuur 1: configuratiescherm 'Netwerk'

Een op die manier geconfigureerde PC zal automatisch een IP-adres aanvragen. Deze aanvraag wordt door de school-router opgevangen, welke ervoor zorgt dat de centrale DHCP-server een IP-nummer zal verstrekken, dat binnen het aan de school toegekende bereik valt.



Figuur 2: configuratiescherm 'TCP/IP'

Dat gaat, zoals gezegd, geheel ongemerkt en automatisch. Het betekent wel dat als de kennisnetaansluiting niet beschikbaar is, er **geen** nummer wordt toegekend.

Voor intern gebruik op het eigen schoolnetwerk zal men dat in de regel niet merken, omdat Windows het laatst toegekende nummer zal blijven gebruiken totdat de geldigheidstermijn verloopt.

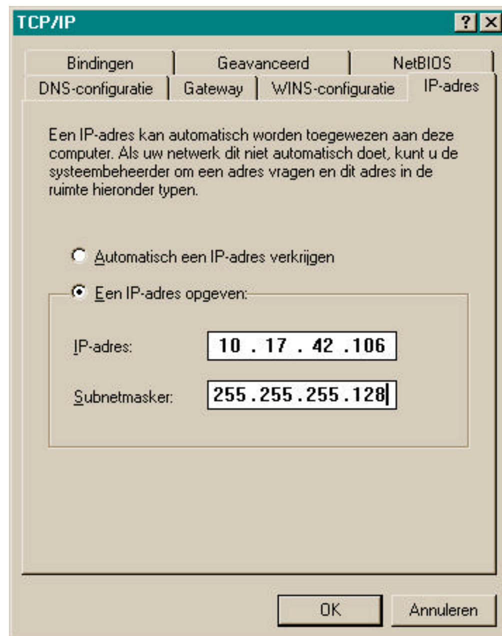
Alleen als de kennisnetaansluiting gedurende langere tijd niet beschikbaar is, kunnen de IP-nummers verlopen, met als gevolg dat men dan ook intern met dat werkstation geen IP meer kan doen.

Door de Golddisk van het Ministerie van Onderwijs, Cultuur en Wetenschappen te gebruiken, wordt de PC automatisch zo ingesteld, dat van DHCP gebruik wordt gemaakt.

1.2 Ik wil graag in Windows een statisch adres opgeven. Hoe doe ik dat?

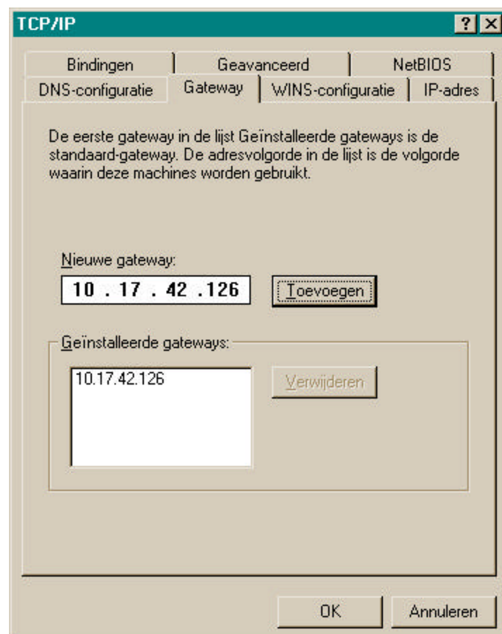
Als het goed is, hebt u van uw kabelmaatschappij of het bedrijf dat uw school op kennisnet heeft aangesloten, een overzicht gehad van de voor u van toepassing zijnde IP-instellingen. Indien dit niet het geval is, kunt u via het Servicepunt kennisnet alsnog uw gegevens opvragen.

Open het configuratiescherm voor TCP/IP. Ga (indien dit niet direct voorkomt) naar het tabblad IP-adres.



Figuur 3: statisch IP-adres

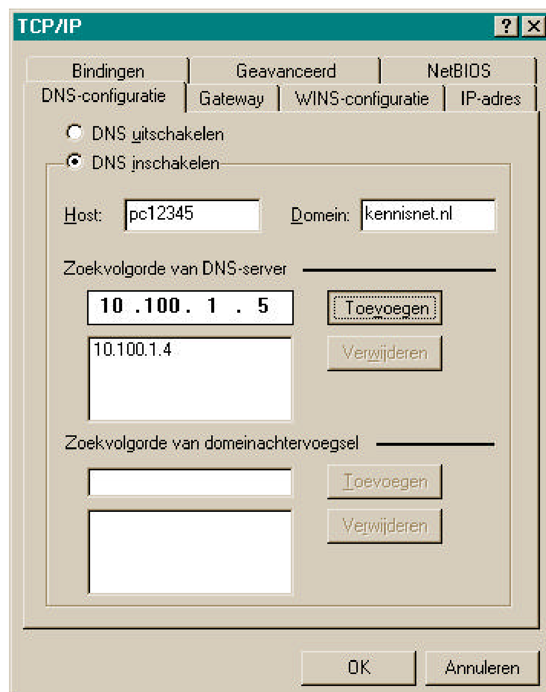
Op het tabblad ‘IP-adres’ dient het vaste adres voor de PC te worden opgegeven. Er moet ook een zogenoemd subnetmasker worden opgegeven. Door het subnetmasker met een rekenkundige bewerking (de zogenoemde binaire 'AND'-operatie) te combineren met het opgegeven IP-adres, weet de computer welke adressen tot het lokale netwerk behoren.



Op het tabblad 'Gateway' dient u het zogenoemde gateway-adres in te stellen. Dit is het IP-adres van uw school-router aan de kant van uw lokale netwerk. Normaal is dit het hoogst of het laagst beschikbare IP-adres uit de aan u toegekende reeks adressen.

Vul het adres van de gateway in onder 'Nieuwe gateway' en klik op 'Toevoegen'. Verwijder eventueel de reeds bestaande 'geïnstalleerde gateways'.

Figuur 4: gateway



Ga naar het tabblad 'DNS-configuratie'. Schakel het gebruik van DNS in. Een aantal velden wordt dan actief.

Achter 'Host:' moet een naam worden ingevuld voor de computer. In principe moet dit een unieke naam zijn, bijvoorbeeld het BRIN- en vestigingsnummer van uw school, de aanduiding 'PC', gevolgd door een volgnummer, zeg `"99ZZ99PC0023"`.

Achter 'Domein:' dient u '`kennisnet.nl`' in te vullen.

Vervolgens dient u de zogenoemde DNS-servers op te geven. Verwijder allereerst eventuele reeds ingevoerde serveradressen. Typ vervolgens het adres '`212.178.5.4`' in, klik op 'Toevoegen' en doe hetzelfde voor '`212.178.5.5`'.

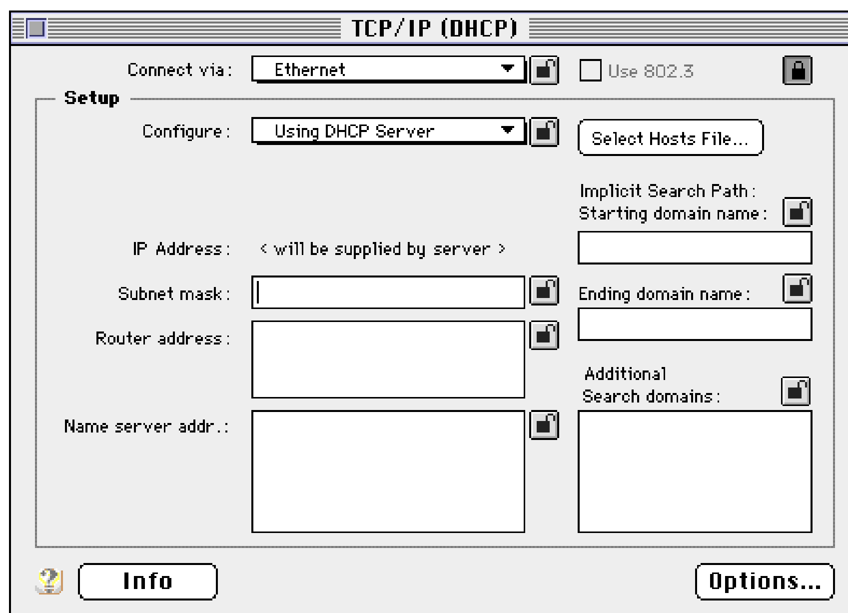
Figuur 5: DNS-configuratie

Overige TCP/IP-instellingen kunt u ongemoeid laten.

1.3 Hoe stel ik de Apple Macintosh in?

MacOS, het besturingssysteem van de Apple Macintosh, kan vanaf versie 7.5, met MacTCP en Open Transport, gebruikmaken van DHCP om automatische IP-instellingen te verkrijgen. Eventueel kunnen deze worden gevonden via de website van Apple: http://www.apple.com. Zoek daar naar 'Open Transport'.

Open het regelpaneel voor TCP/IP. Maak indien nodig een nieuwe configuratie aan, bijvoorbeeld met de naam 'kennisnet'.



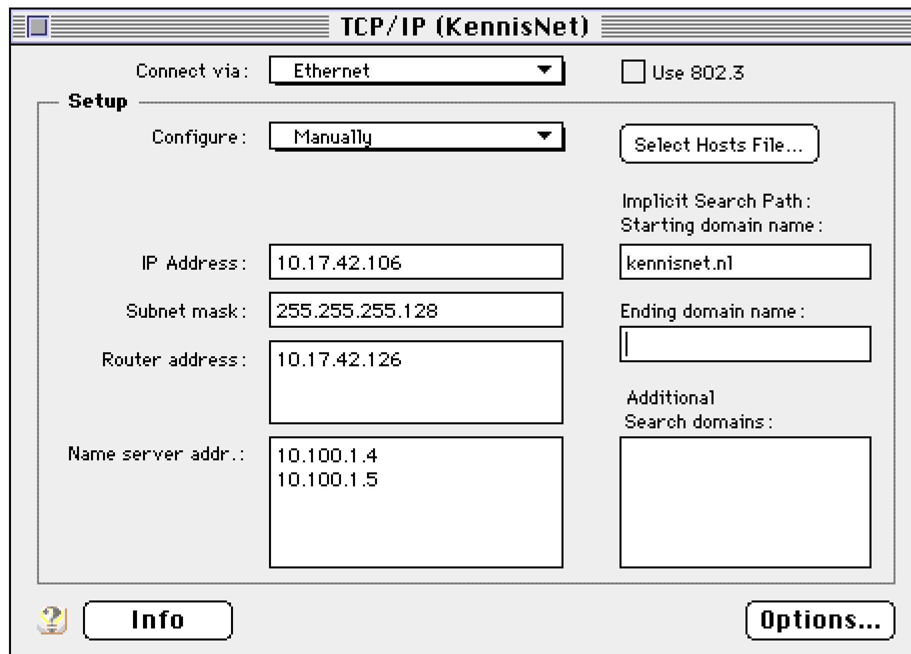
Figuur 6: regelpaneel TCP/IP-configuratie

Selecteer achter 'Connect via' de optie 'Ethernet'. Selecteer dan achter 'Configure' de optie 'via DHCP'. Verder worden alle opties door de server ingevuld. Bewaar deze configuratie en maak deze actief.

Let op dat MacOS bij het herstarten van de computer of bij het ontwaken uit sluimerstand de verkregen gegevens weggooit en ververst. Als er dus geen verbinding met kennisnet is, zal na het verlopen van de geldigheidsduur de computer niet meer via TCP/IP kunnen werken. De geldigheidsduur van de gegevens is echter vrij lang.

1.4 Ik wil graag in MacOS een statisch adres opgeven. Hoe doe ik dat?

Start het regelpaneel 'TCP/IP'. Open de lijst met configuraties (command-K). Maak een nieuwe configuratie (bijvoorbeeld door er een te dupliceren) of selecteer een te wijzigen configuratie en maak deze actief. U keert dan terug naar het regelpaneel.



Figuur 7: statische IP-configuratie MacOS

Achter 'Connect via:' dient u 'Ethernet' te selecteren. Aangezien alle instellingen nu handmatig worden gedaan, selecteert u achter 'Configure:' de optie 'Manually'. Vul vervolgens het IP-adres van de computer in en het subnetmasker. Het adres van de router is normaal gesproken het hoogste of het laagste adres uit de aan u toegekende reeks. Deze gegevens zou u van uw kabelmaatschappij ontvangen moeten hebben. Eventueel kunt u deze opvragen via het Servicepunt kennisnet.

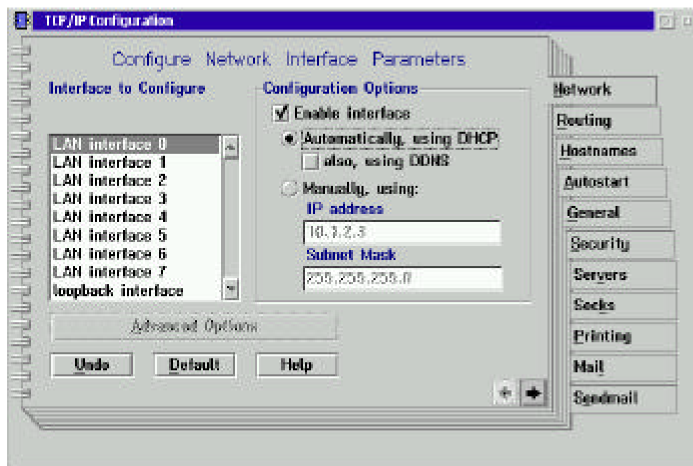
In alle gevallen kunt u bij 'Name server addr.' invullen `212.178.5.4`' en '`212.178.5.5`'. De domeinnaam onder 'Starting domain name' dient '`kennisnet.nl`' te zijn.

Sluit het venster en bevestig de wijzigingen.

1.5 Kan ik met OS/2 Warp op kennisnet?

Ja, met OS/2 Warp 3.0 of hoger, uit de blauwe doos (niet de rode!), ook wel bekend als 'Warp Connect' (versie 3) en 'Merlin' (versie 4), kunt u gebruikmaken van TCP/IP en daarmee van kennisnet en het Internet. Uiteraard dient u ondersteuning voor TCP/IP geïnstalleerd te hebben. In dit voorbeeld is de 'UK'-versie (Brits Engels) van OS/2 Warp 4 gebruikt.

Om gebruik te maken van DHCP, gaat u als volgt te werk. Open het 'System Setup'-venster. Kies dan 'TCP/IP Configuration (LAN)'. Ga dan naar het eerste tabblad met de titel 'Network'.



Figuur 8: OS/2 TCP/IP-configuratie via DHCP

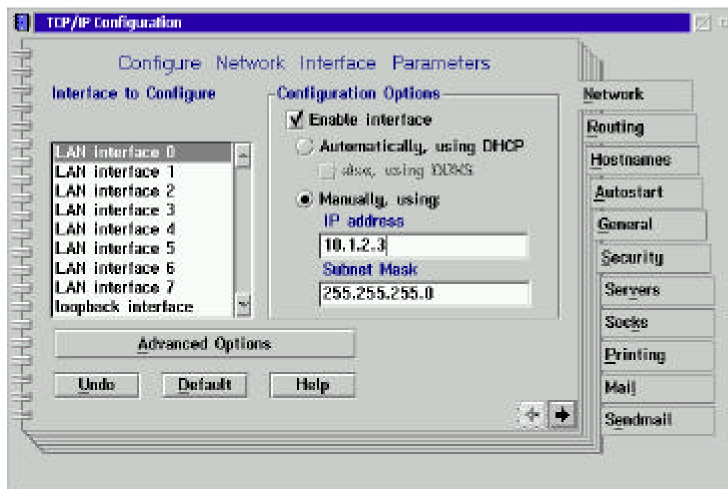
Op het eerste tabblad kiest u de betreffende interface, doorgaans 'LAN interface 0' voor de eerste ethernet-aansluiting.

Selecteer vervolgens 'Enable Interface' en kies 'Automatically, using DHCP'.

Sluit vervolgens het venster en bevestig dat u de wijzigingen wilt opslaan. Volgens de instructies dient u nu uw computer te herstarten om de nieuwe instellingen in werking te doen treden. Meer ervaren gebruikers kunnen ook zonder herstart verder werken; dit is, voorzover bekend, echter ongedocumenteerd.

1.6 Kan ik met OS/2 Warp een statisch IP-adres instellen?

Ja, dat kan. Dit is iets meer werk dan met DHCP, maar het is mogelijk. Open het venster 'TCP/IP Configuration (LAN) uit de 'System Setup'. Ga naar het eerste tabblad, met de naam 'Network'.



Figuur 9: OS/2 handmatige TCP/IP-configuratie

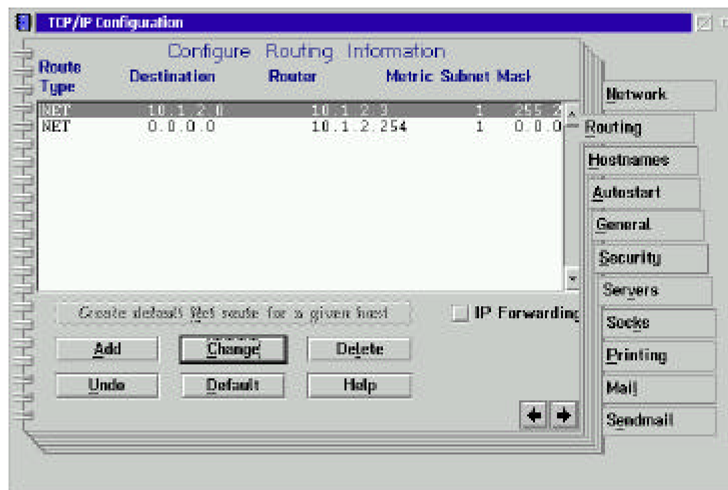
Op het eerste tabblad kiest u de betreffende interface, doorgaans 'LAN interface 0' voor de eerste ethernet-aansluiting.

Selecteer vervolgens 'Enable Interface' en kies 'Manually using:'. Vul het IP-adres van de machine in en vervolgens het netwerkmasker.

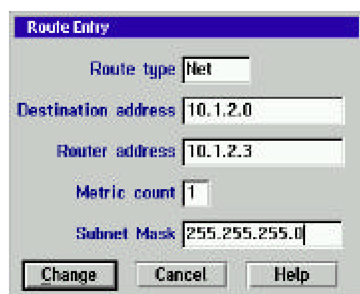
Ga door naar het tabblad 'Routing'.

Op het tabblad 'Routing' kunt u routes instellen om het verkeer in goede banen te leiden. Normaliter stelt u op een werkstation slechts twee routes in:

- de route naar het lokale netwerk;
- de 'default'-route, ofwel de weg naar de rest van de wereld.



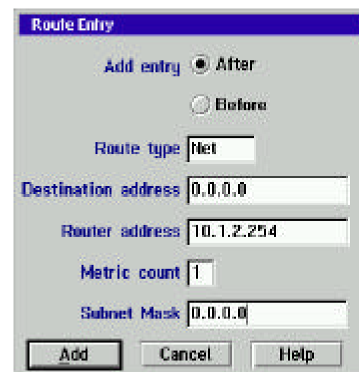
Figuur 10: OS/2 IP-routes



Figuur 11: lokaal netwerk

Allereerst stelt u de route naar het lokale netwerk in. Klik op 'Add' en in het venster dat dan verschijnt, geeft u het netwerkadres, het adres van de router (in dit geval het IP-adres van *deze* machine), ‘Metric count’ is 1 en tenslotte vult u het netwerkmasker in. Klik op 'Change' of 'Add'.

Klik weer op 'Add'. Selecteer in het venster 'After'. Geef als 'Destination address' vier nullen ('0.0.0.0'), vul het adres van de router in, wederom ‘Metric count’ is 1 en als netwerkmasker weer vier nullen ('0.0.0.0'). Klik op 'Change' of 'Add'



Figuur 12: default-route

Indien de OS/2-machine als router wordt gebruikt (bijvoorbeeld tussen uw lokale netwerk en kennisnet), kunt u eventueel de optie 'IP Forwarding' selecteren, zodat IP-verkeer door de machine kan worden gerouteerd. Hiervoor dienen echter ook meerdere ethernet-interfaces beschikbaar te zijn.

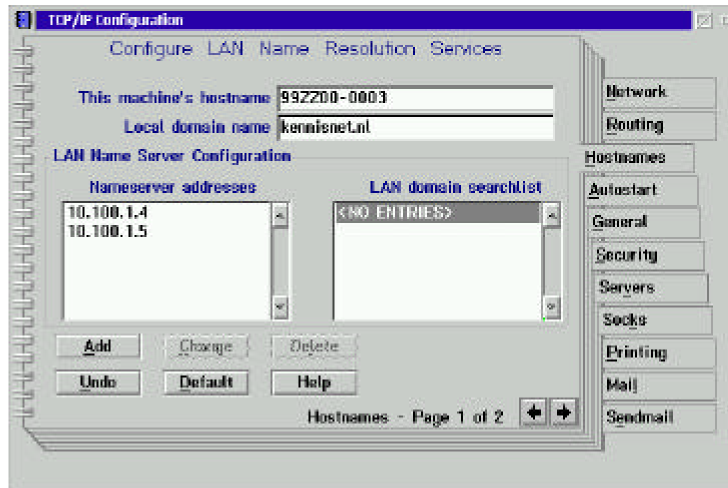


Figuur 13: OS/2 IP Forwarding

Ga daarna naar het tabblad 'Hostnames', dat uit twee pagina's bestaat.

Op de eerste pagina kunt u de naam en het domein van de machine opgeven. Middels de knop 'Add' kunt u, wanneer u de lijst 'Nameserver addresses' aanklikt, de adressen van de DNS-servers opgeven, namelijk '212.178.5.4' en '212.178.5.5'

Op de tweede bladzijde van het tabblad kunt u eventueel namen van lokale machines of van machines waar veel contact mee is, opnemen in een lijst.



Figuur 14: OS/2 Hostname

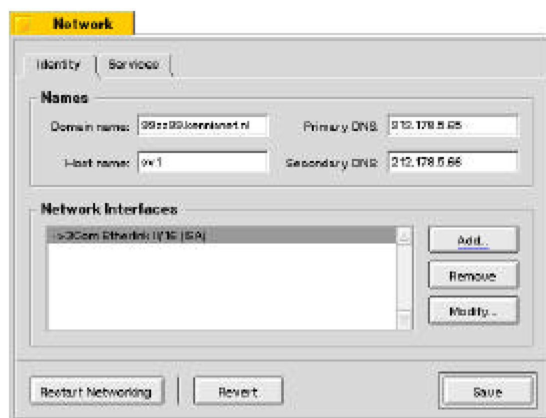
Sluit het venster en bevestig dat u de wijzigingen wilt doorvoeren. Volgens de documentatie dient u nu uw computer te herstarten om de nieuwe instellingen actief te maken. Ervaren gebruikers kunnen ook zonder herstarten van de opties gebruikmaken; dit is, voorzover bekend, echter ongedocumenteerd.

1.7 Kan ik met BeOS gebruikmaken van kennisnet?

Zoals ieder ander besturingssysteem dat het Internetprotocol ondersteunt, kan ook met BeOS gebruik worden gemaakt van kennisnet. Dit is overigens veel sterker afhankelijk van de vraag of uw hardware in voldoende mate wordt ondersteund. Raadpleeg hiervoor de website van Be, `http://www.be.com/`.

Om BeOS in te stellen voor kennisnet, gaat u als volgt te werk. Open de 'Preferences' en selecteer 'Network'.





Figuur 15: BeOS-netwerkinstellingen

Er verschijnt een venster met twee tabbladen. Met name het eerste tabblad is van belang voor de instellingen voor kennisnet. U vult hier de domein- en machinenaam in achter 'Domain name', respectievelijk 'Host name'. Uw domeinnaam is hier het BRIN-nummer van uw school + het vestigingsnummer, gevolgd door '`.kennisnet.nl`'.

U kunt hier tevens de primaire en secundaire DNS-servers opgeven: dit zijn `212.178.5.4`, respectievelijk `212.178.5.5`. Dit hoeft u *niet* in te vullen wanneer u via DHCP een adres verkrijgt!

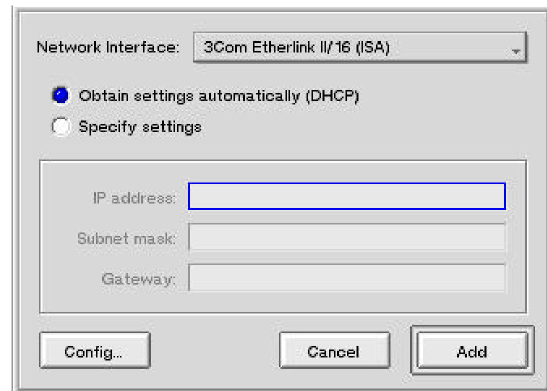
Afhankelijk van of u reeds een netwerk geïnstalleerd hebt, dient u vervolgens op 'Add' (toevoegen) of 'Modify..' (aanpassen) te klikken om uw netwerkaansluiting in te stellen.

Selecteer in de keuzebalk de juiste netwerkkaart.

Standaard staat het systeem al ingesteld op het gebruik van DHCP, opdat het systeem automatisch een IP-adres toegewezen krijgt.

Klik op 'Add' om de netwerkaansluiting toe te voegen, resp. 'Modify..' om de aangepaste instellingen op te slaan.

In het venster van Figuur 15 klikt u vervolgens op de knop 'Restart Networking' om de nieuwe instellingen te activeren. Klik op 'Save' om alles te bewaren.



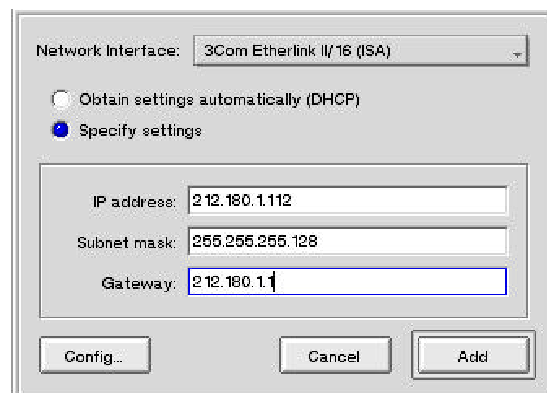
Figuur 16: BeOS DHCP

1.8 Hoe stel ik in BeOS een statisch IP-adres in?

Ga, zoals in paragraaf 1.7 beschreven, naar de 'Network Preferences' en voeg een netwerkaansluiting toe of wijzig de bestaande aansluiting. U krijgt wederom het venster dat in Figuur 16 is getoond. Selecteer nu, zoals in Figuur 17, de optie 'Specify settings'. De velden in het kader worden geactiveerd.

Vul uw IP-adresgegevens in. Eerst het IP-adres van de machine achter 'IP address', gevolgd door het netwerkmasker achter 'Subnet mask' en tenslotte het adres van de router achter 'Gateway'.

Klik dan op 'Add' of 'Modify..' om de instellingen door te voeren. Klik dan 'Restart Networking' om de instellingen te activeren. Klik op 'Save' om de instellingen op te slaan.



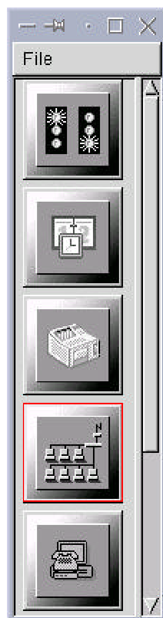
Figuur 17: BeOS statisch IP-adres

1.9 Hoe kan ik Linux instellen voor het gebruik van kennisnet?

Deze vraag is wat lastiger te beantwoorden dan bij de andere besturingssystemen. Niet omdat het zoveel moeilijker is, maar omdat vrijwel iedere distributie haar eigen hulpmiddelen heeft. Er zullen daarom drie distributies besproken worden: RedHat 6.x, Slackware, SuSe (in alfabetische volgorde). U dient zich in alle gevallen als 'root' aan te melden, omdat de handelingen dit vereisen.

1.9.1 RedHat

Bij RedHat Linux is het configureren van het netwerk met of zonder DHCP weinig verschillend van elkaar. Daarom wordt dit als één geheel behandeld.



Figuur 18: Control Panel

Open het Control Panel en klik op de Network Configurator. Er verschijnt een venster, zoals in Figuur 19. Hier kunt u het systeem een hostnaam en een domeinnaam geven. In dit voorbeeld wordt een werkstation ingesteld in een schoolsituatie. Als domein wordt het domein van de school (99ZZ99.kennisnet.nl) gebruikt. Daarnaast kan voor zoeken naar domeinen bijvoorbeeld 'kennisnet.nl' extra worden opgegeven. U dient verder IP-adressen van de DNS-servers op te geven. Dit zijn 212.178.5.4 en 212.178.5.5.

Indien u DHCP wilt gebruiken, dient u de DNS-server *niet* in te vullen en kunt u eventueel de domeinnamen achterwege laten. Klik op 'Save' om de wijzigingen te bewaren.

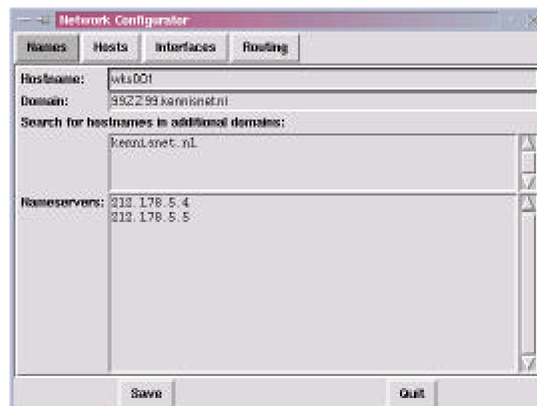
Op de pagina 'Hosts' kunt u statische IP-adressen aan namen koppelen. U dient in ieder geval de koppeling van 127.0.0.1 aan 'localhost' te behouden (deze is standaard ingevuld). Indien u DHCP gebruikt, kunt u de lijst verder laten voor wat deze is. Anders kunt u in elk geval het IP-adres van de betreffende machine aan de naam koppelen.



Figuur 21: RedHat, toevoegen host

Op de pagina 'Interfaces' kunt u alle netwerk-interfaces invoeren die u op uw systeem hebt. U hebt standaard altijd de interface 'lo' (local) met het IP-adres 127.0.0.1. Deze dient u **altijd** te laten staan! Met de knop 'Add' kunt u eventuele extra interfaces toevoegen.

Voor bijvoorbeeld een ethernet-interface (meestal `eth0`) kunt u, zoals hieronder, de gegevens ingeven.

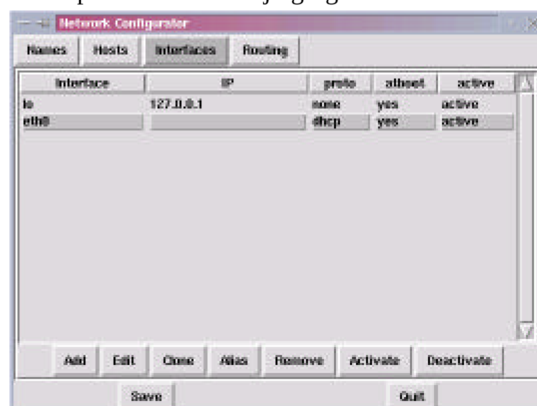


Figuur 19: RedHat, Network Names



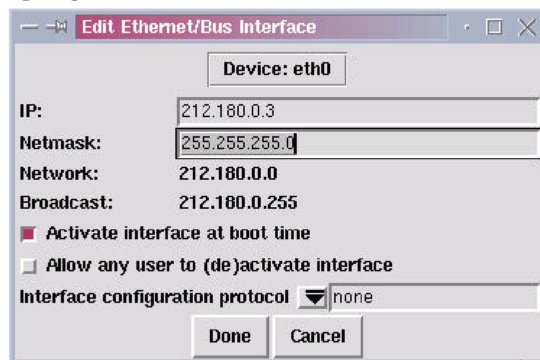
Figuur 20: RedHat, Hosts

Klik op de knop 'Add' om een 'host' toe te voegen. Geef het IP-adres. Achter 'Name:' vult u de volledige naam van de machine (host + domein) in en achter 'Nicknames:' geeft u de verkorte naam (alleen de hostnaam). Klik dan op 'Done'. Klik op 'Save' om de wijzigingen te bewaren.



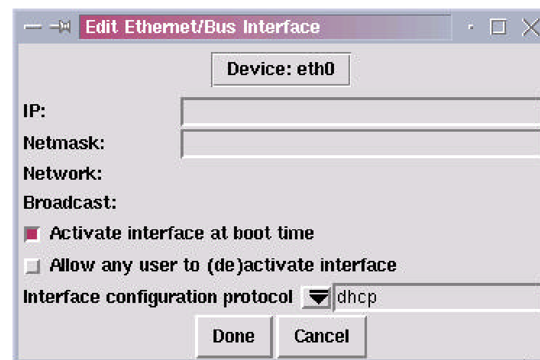
Figuur 22: RedHat, netwerk-interfaces

Statische adressering. Wanneer u gebruikmaakt van vaste adressen, vult u achter 'IP:' het IP-adres van de machine in. Daaronder geeft u het netwerkmasker op. Waarschijnlijk kunt u 'Activate interface at boot time' ingeschakeld laten, zodat de netwerkkaart wordt ingeschakeld bij het starten van het systeem. Achter 'Interface configuration protocol' dient u 'none' (standaard) op te geven.



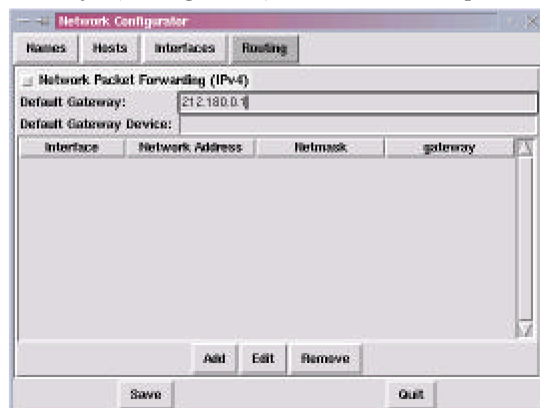
Figuur 23: RedHat, nieuwe interface, statisch

Dynamische adressering. Wanneer u gebruik wilt maken van DHCP of BOOTP, laat u het IP-adres en het netwerkmasker (Netmask) leeg. Laat de optie 'Activate interface at boot time' ingeschakeld en achter 'Interface configuration protocol' dient u 'dhcp' te selecteren voor DHCP en 'bootp' voor 'BOOTP'.



Figuur 24: RedHat, nieuwe interface, DHCP of BOOTP

Sluit het venster door op 'Done' te klikken. Vervolgens kunt u de netwerkkaart inschakelen door deze in de lijst (zie Figuur 22) te selecteren en op de knop 'Activate' te klikken.



Figuur 25: RedHat, Routing

Op de pagina 'Routing' voltooit u de netwerkconfiguratie door achter 'Default Gateway:' het adres van de router in te vullen. Tenzij u geen andere specifieke routes hebt, kunt u de rest leeg laten.

Klik op 'Save' om de wijzigingen te bewaren en klik op 'Quit' om de configuratie af te sluiten.

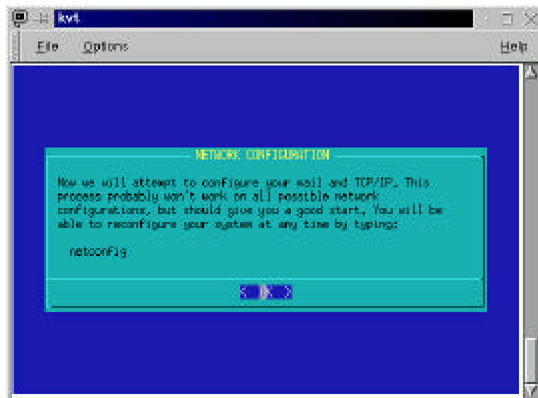
Sluit, wanneer u klaar bent, het Control Panel af.

Normaliter zou de netwerkinterface nu gereed moeten zijn en functioneren. Indien dit niet het geval is, kunt u met het onderstaande commando alsnog de nieuwe configuratie activeren:

```
/etc/rc.d/init.d/network restart
```

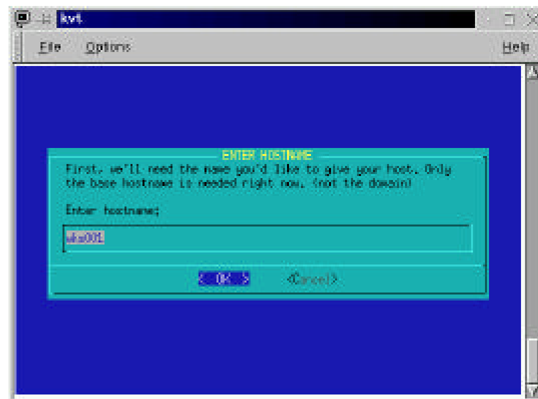
1.9.2 Slackware

Onder Slackware start u, indien u dit nog niet tijdens de installatie hebt gedaan, de netwerkconfiguratie met de opdracht '`/sbin/netconfig`'. U wordt door middel van een aantal schermen door de configuratie geleid. Slackware biedt geen mogelijkheid om DHCP-gebruik te configureren. Aan het einde van de Slackware-configuratie volgen nog enkele tips.



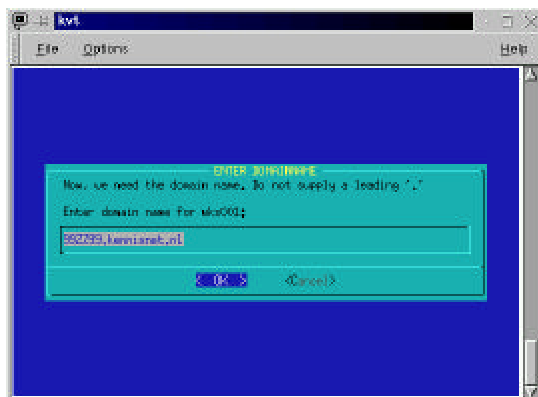
Figuur 26: Slackware start netwerkconfiguratie

In het eerste scherm wordt enige korte uitleg gegeven over de configuratie die u gaat uitvoeren. Druk op 'Enter' om verder te gaan.



Figuur 27: Slackware hostnaam

In het tweede scherm wordt u gevraagd om een hostnaam, *zonder* domein en *zonder* punt erachter, in te voeren. Typ de naam en druk op 'Enter' om verder te gaan.



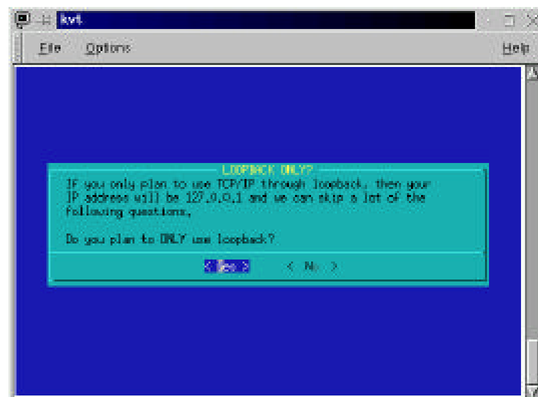
Figuur 28: Slackware domeinnaam

In het derde venster dient u de domeinnaam, *zonder* voorafgaande punt, in te vullen.

Daarna krijgt u de vraag of u uitsluitend gebruik wilt maken van 'loopback'. Wanneer u hier 'Yes' antwoordt, bent u verder klaar met de configuratie, maar zijn er verder geen adresgegevens ingevoerd. U kunt hier 'Yes' antwoorden indien u:

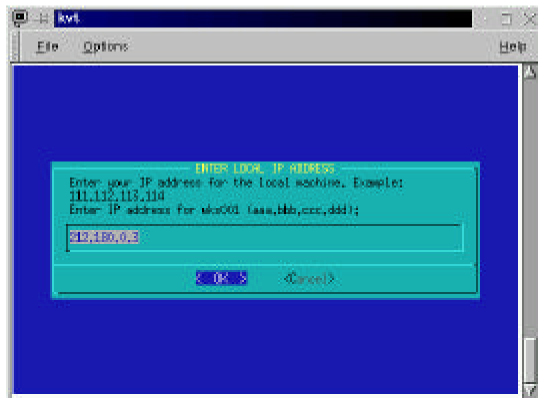
- de computer niet op het netwerk aansluit via ethernet;
- gebruik wilt maken van DHCP[1].

In andere gevallen kiest u 'No' (met de tab-toetsen) en drukt u op 'Enter'.



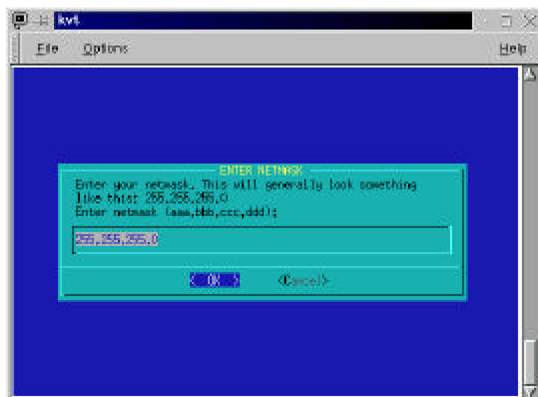
Figuur 29: Slackware 'Only use loopback?'

[1] Indien u DHCP wilt gebruiken, hoeft u geen verdere instellingen op te geven. Een DHCP-programma stelt alle gegevens verder in.



Figuur 30: Slackware IP-adres

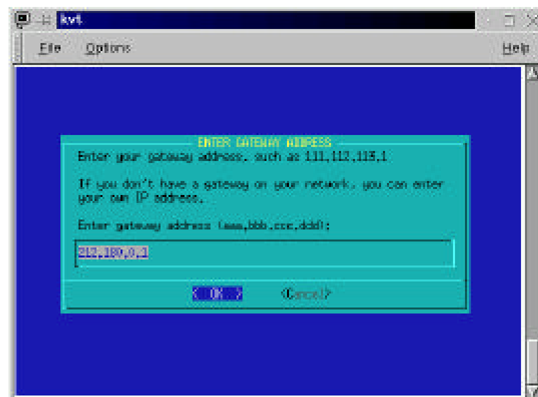
Daarna vult u het adres van de 'default gateway' in. Dit is het adres van de kennisnet-router. Indien u geen gebruik wilt maken van de default gateway (bijvoorbeeld voor als u de machine alleen op het lokale netwerk gebruikt en *niet* daarbuiten), dan dient u hier het IP-adres van deze machine zelf in te vullen.



Figuur 32: Slackware netwerkmasker

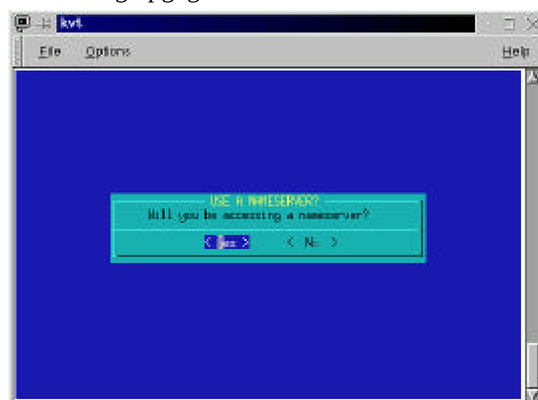
U krijgt vervolgens de vraag of u gebruik wilt maken van een nameserver. U dient hier 'Yes' te antwoorden en op 'Enter' te drukken.

Wanneer u 'Yes' hebt geantwoord op de voorgaande vraag, dient u in het vijfde venster het IP-adres van de machine in te vullen. Druk vervolgens op 'Enter'.

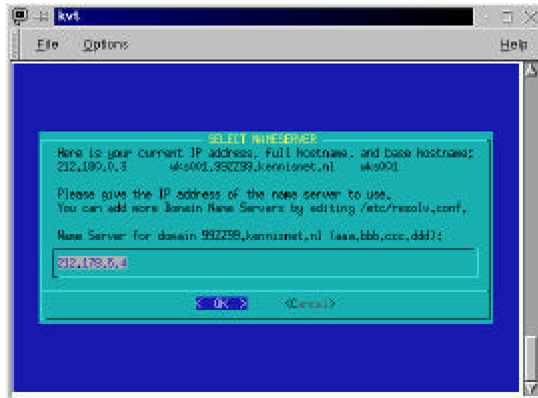


Figuur 31: Slackware Gateway

In het achtste scherm dient u het netwerkmasker in te vullen. Dit ziet er bijvoorbeeld uit als '255.255.255.0'. Het werkelijke masker krijgt u bij aansluiting opgegeven.



Figuur 33: Slackware ‘Use a Nameserver?’



U dient het adres van één nameserver in te vullen: 212.178.5.4. Wanneer u ook de andere nameserver wilt invoeren, dient u met de hand het bestand '`/etc/resolv.conf`' aan te passen; kopieer de regel '`nameserver 212.178.5.4`' en vervang het IP-adres door `212.178.5.5`.

Figuur 34: Slackware nameserver-adres

Om de nieuwe configuratie in werking te doen treden, dient u het script `/etc/rc.d/rc.inet1` te starten met de opdracht '`sh /etc/rc.d/rc.inet1`'.

Tips voor gebruik van DHCP onder Slackware:

- Software
  - U kunt het DHCP-pakket van ISC (The Internet Software Consortium) ophalen (van `http://www.isc.org/`) en de 'client' dhclient gebruiken.
  - U kunt het programma 'pump' opzoeken en installeren.
- U dient in `/etc/rc.d/rc.inet1`, aan het einde, of in `/etc/rc.d/rc.inet2` één of enkele regels op te nemen om de DHCP-client te starten, bijvoorbeeld:

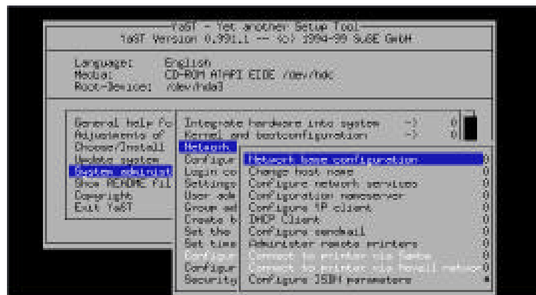
```
if [ -x /sbin/dhclient ]; then
  /sbin/dhclient eth0
fi
```

of

```
if [ -x /sbin/pump ]; then
  /sbin/pump -i eth0
fi
```

1.9.3 SuSe

SuSe gebruikt voor vrijwel alle te configureren opties het programma 'YaST'. U start dit door simpelweg de opdracht '`yast`' te geven op de commandoregel. In SuSe is er een vrij sterk verschil in de configuratie met en zonder DHCP. In beide gevallen start u echter eerst 'YaST' op.



Figuur 35: YaST

Nadat u YaST hebt opgestart, komt u in het hoofdmenu.

Kies 'System administration' en vervolgens 'Network configuration'. Hier kunt u kiezen hoe u verder wilt: statische IP-adressering of DHCP gebruiken.

In beide gevallen zult u echter een machinenaam willen opgeven. Kies hiervoor 'Change host name'.

U krijgt het venster in Figuur 36 te zien. Achter 'Hostname' vult u de naam van de machine in, bestaande uit cijfers, letters en eventueel een streepje.

Acter 'Domain name' geeft u de domeinnaam. Met 'Tab' gaat u verder naar de knop '<Continue>'.



Figuur 36: YaST, Change hostname

Statische adressering



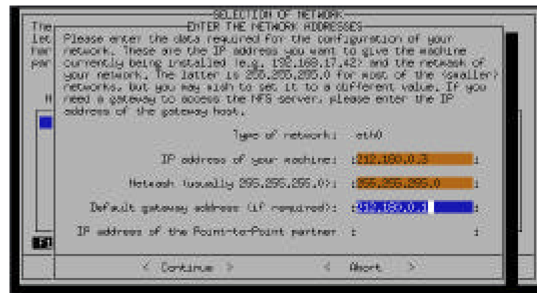
Figuur 37: YaST, Base Network Configuration

Om een statisch adres in te stellen, kiest u 'Base network configuration[2] en krijgt u een venster zoals in Figuur 37. U kunt hier iedere interface in uw systeem configureren. In dit voorbeeld wordt uitgegaan van alleen `eth0`, de ethernet-kaart op positie 0. Druk op F5 om een netwerkkaart aan te maken (kies Ethernet) en vervolgens op F6 om de IP-gegevens in te stellen.

[2] Indien u al gebruikmaakt van DHCP, dient u dat eerst uit te schakelen om 'Base network configuration' te kunnen gebruiken. Dit gaat analoog aan het inschakelen.

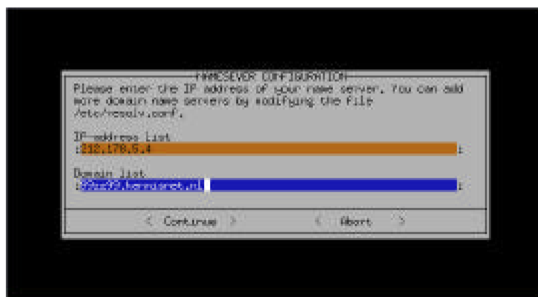
Geef achter 'IP address of your machine' het IP-adres, en het netwerkmasker achter 'Netmask'[3]. Vul achter 'Default gateway address' het adres van uw router in. Indien u de betreffende machine als afgeschermde server wilt gebruiken (dus geen verbinding met kennisnet), dan kunt u dit veld leeg laten.

Ga met 'Tab' van het ene naar het andere veld en klik op '<Continue>' om het venster te sluiten en de opties vast te leggen.



Figuur 38: YaST, statisch IP-adres

Vervolgens kiest u 'Configure nameserver'. U wordt gevraagd of u gebruik wilt maken van een nameserver. Kies 'Yes' en druk op ‘Enter’ om verder te gaan. U kunt één nameserver-adres (212.178.5.4) opgeven en een domeinnaam. Deze domeinnaam kan `kennisnet.nl`' zijn of de lokale domeinnaam voor uw LAN (<BRIN+vestiging>+'`.kennisnet.nl`'). Kies '<Continue>' om de gegevens vast te leggen.



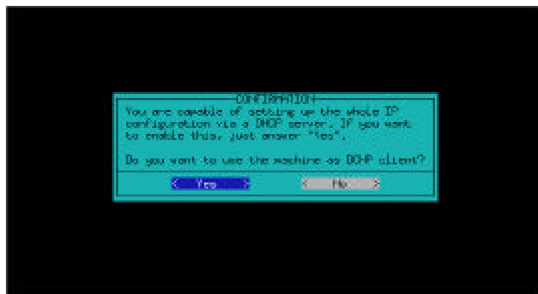
Figuur 39: YaST, Nameservers

Hiermee is de configuratie compleet. Druk enkele malen op 'Esc' om YaST te verlaten. Om de nieuwe configuratie in te stellen, typt u:

```
/etc/rc.d/network start; /etc/rc.d/route start
```

Met name wanneer u dit van afstand (via telnet of secure shell) doet, is het belangrijk dat u dit als één commando doet.

DHCP



Kies uit het menu 'DHCP client'. U krijgt de vraag of u uw machine als DHCP-client wilt gebruiken. Indien ja, kies 'Yes' en druk op ‘Enter’. De instellingen worden vervolgens aangepast.

Figuur 40: YaST, DHCP-configuratie

Hiermee is de configuratie compleet. Druk enkele malen op 'Esc' om YaST te verlaten. Om de nieuwe configuratie in te stellen typt u:

```
/etc/rc.d/network start; /etc/rc.d/route start; /etc/rc.d/dhcp start
```

Dit commando kunt u beter niet via telnet of secure shell uitvoeren. U dient dit op de machine zelf (console of terminalvenster) te doen.

[3] Er staat achter 'Usually 255.255.255.0'. Dit gaat alleen maar op voor zogenoemde klasse C-netwerken, van 256 adressen. Op kennisnet worden adresreeksen van 32 t/m 1024 adressen gebruikt. Gebruik dus het netwerkmasker dat u bij aansluiting of bij de IP-migratie hebt opgekregen.

1.10 Wij gebruiken Windows 3.1x en dat ondersteunt geen DHCP. Wat nu?

U hebt in dit geval vier opties.

- Windows 3.11 (Windows for Workgroups) kan geschikt worden gemaakt voor TCP/IP en DHCP. Op het adres ftp://ftp.microsoft.com/bussys/clients/wfw/ is een 32bits versie van de MS TCP-stack beschikbaar (TCP32B). U dient **niet** het pakket TCPWFW te selecteren! Aan het einde van deze paragraaf wordt uitgelegd hoe u TCP32B kunt installeren.
- U kunt, indien de hardware dit toelaat, uw systemen opwaarderen naar Windows 95/98/NT of Win-OS/2 (OS/2 Warp 3 of 4, 'blue box') en zo toch gebruikmaken van DHCP.
- U kunt al uw werkstations handmatig adressen toekennen.
- U kunt zelf een BOOTP-server opzetten en DHCP voor uw IP-reeks laten uitschakelen. Zie deel V voor meer informatie. De DHCP-server van 'the Internet Software Consortium' (http://www.isc.org) biedt ook BOOTP-functionaliteit en is redelijk eenvoudig qua installatie en onderhoud.

Raadpleeg het Servicepunt kennisnet indien u zelf een BOOTP-server wilt opzetten of indien u nog aanvullende vragen hebt.

1.10.1 Installatie TCP32B voor Windows 3.1x.

Haal het bovengenoemde bestand op (eventueel met behulp van een ander systeem) voor installatie. Start Windows en open de Hoofdgroep ('Main'). Pak het bestand uit in een map, die u eenvoudig kunt vinden, bijvoorbeeld `C:\TEMP`.



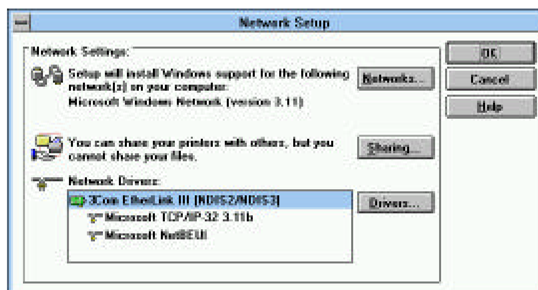
Figuur 41: Hoofdgroep/Main

Klik op het icoontje voor de 'Windows Setup'. Dan verschijnt een klein venster.



Figuur 42: Windows Setup

Seleteer 'Netwerkconfiguratie' of 'Change Network Settings...' uit het menu zoals getoond.



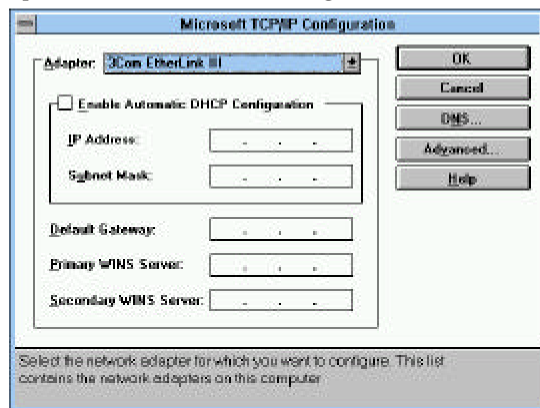
Figuur 43: netwerkconfiguratie

In het venster voor de netwerkconfiguratie kunt u soorten netwerken installeren. Mogelijk dient u uw bestaande stuurprogramma's voor TCP/IP eerst te verwijderen. Selecteer uw netwerkkaart en klik op 'Drivers...'/'Stuurprogramma's'.

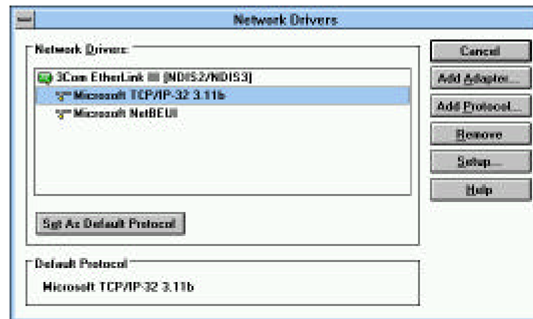
Om eventuele bestaande stuurprogramma's voor TCP/IP te verwijderen, selecteert u het protocol en klikt u op 'Verdwijderen'/'Remove'. Bevestig uw keuze. Laat andere netwerkprotocollen intact!

Klik vervolgens op 'Protocol toevoegen'/'Add Protocol...'. Selecteer uit de lijst 'Unlisted or updated protocol' of het Nederlandstalige equivalent en klik op 'OK'. U dient dan via de knop 'Browse'/'Bladeren' de map op te zoeken waar de software staat. Klik dan op 'OK'.

Selecteer nu het gevonden protocol en klik weer op 'OK'. De installatie wordt gestart.



Figuur 45: TCP/IP-configuratie



Figuur 44: stuurprogramma's

Na de installatie wordt gevraagd om IP-adressen. U kunt er op dat moment ook voor kiezen om DHCP te gebruiken.

Eventueel kunt u het venster weer terugvinden via de netwerkconfiguratie, zoals in Figuur 44, via de knop 'Instellingen'/'Setup'. U kunt dan eventueel uw instellingen aanpassen.

Na de installatie dient u Windows opnieuw te starten.

1.11 Een eigen DHCP-service

In deel V van Het Handboek wordt uitgelegd hoe u dient te handelen indien u zelf voor DHCP wilt zorgen.

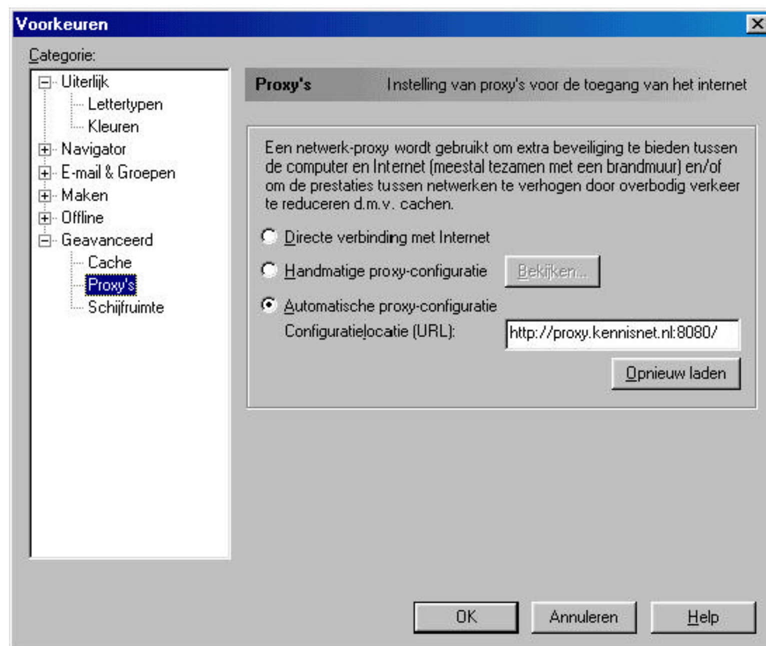
1.12 Wat moet ik instellen in Netscape Communicator?

Met Netscape Communicator kan worden gesurft over het WWW en naar FTP-sites, maar ook kunnen hiermee e-mail en nieuws (discussiegroepen) worden gelezen. Deze toepassingen zullen stuk voor stuk aan bod komen.

1.12.1 Surfen met Netscape Communicator

Om te kunnen surfen op kennisnet en het Internet, moet de 'proxy'-configuratie worden ingesteld. De proxy is in grote lijnen een machine die het netwerkverkeer controleert en beveiligt tegen indringers van buitenaf. Via de proxy kunt u wel naar buiten, maar kunnen anderen niet naar binnen.

De exacte instellingen voor de proxy worden automatisch aangeleverd, maar hiervoor moet wel het adres worden opgegeven.

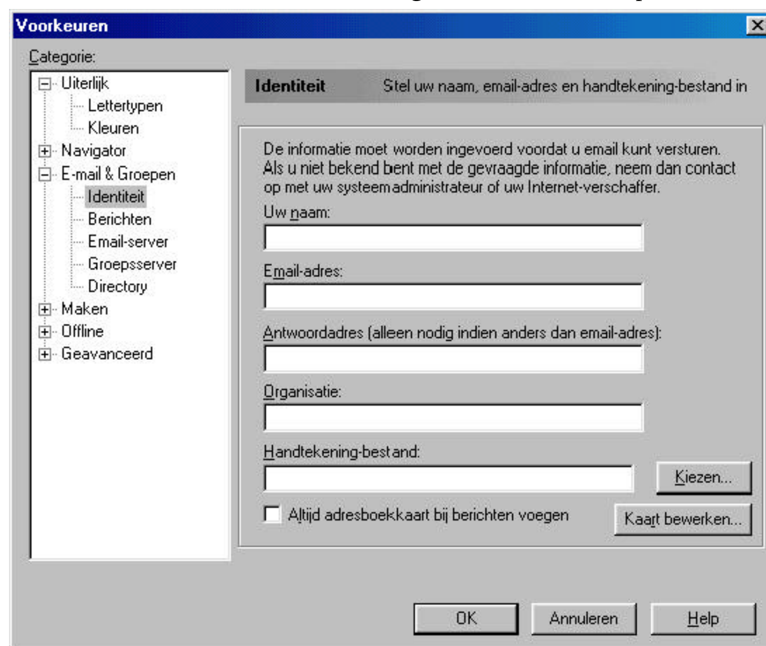


Figuur 46: configuratiescherm, proxy -instellingen

Stel de proxyconfiguratie in op 'Automatische proxy-configuratie' en vul als URL in: `http://proxy.kennisnet.nl:8080/`.

1.12.2 Uw identiteit instellen in Netscape Communicator

Kies in het voorkeurenvenster de categorie 'E-mail & Groepen', sub 'Identiteit'.

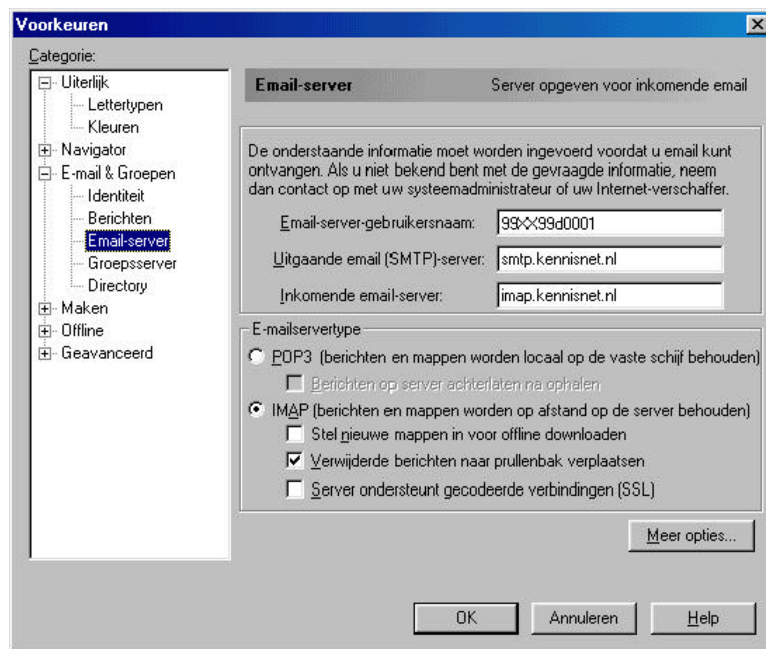


Figuur 47: configuratiescherm, identiteit

Vul hier eventueel uw eigen naam in. Vul in ieder geval het toegewezen e-mailadres (dit is de gebruikersnaam met daarachter '`@kennisnet.nl`') in. Het antwoordadres kan leeg blijven, daar dit hetzelfde is als het e-mailadres. Vul in het vak 'Organisatie' de naam van uw school in.

1.12.3 E-mailinstellingen met Netscape Communicator

Kies in het voorkeurenvenster de categorie 'E-mail & Groepen', sub 'Email-server'.

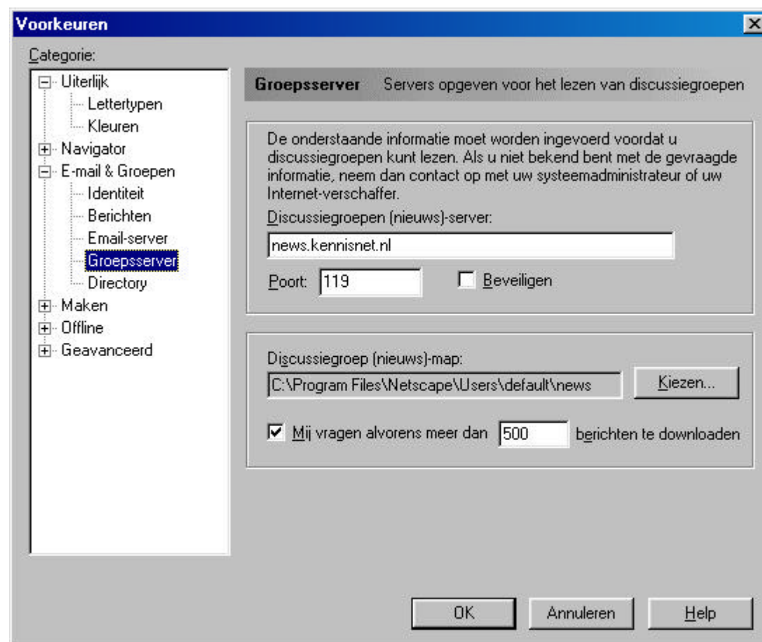


Figuur 48: voorkeuren e-mail-server

Achter "Email-server-gebruikersnaam" vult u uw gebruikersnaam voor kennisnet in. De server voor uitgaande mail is `smtp.kennisnet.nl`. De server voor inkomende mail is, hetzij `pop.kennisnet.nl` (indien voor het POP3-protocol wordt gekozen), hetzij `imap.kennisnet.nl` (indien voor het IMAP4-protocol wordt gekozen). Zie deel VIII (Begrippenlijst) om te kunnen bepalen welke van de twee protocollen voor uw situatie de beste is.

1.12.4 Discussiegroepenmet Netscape Communicator

Om van discussiegroepen gebruik te kunnen maken, dient u de 'groepsserver' in te stellen. Kies in het voorkeurenvenster de categorie 'E-mail & Groepen', sub 'Groepsserver'.



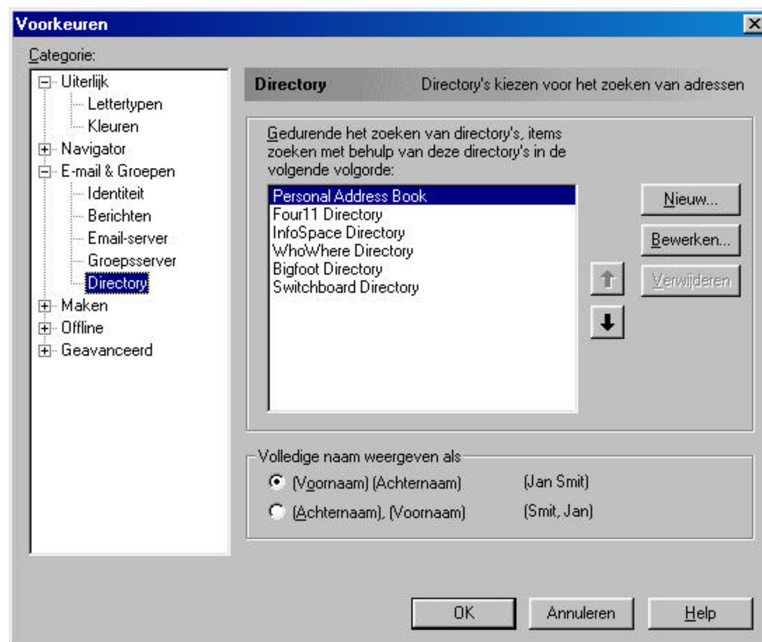
Figuur 49: voorkeuren groepsserver

Vul bij 'Discussiegroepen (nieuws)-server:' in '`news.kennisnet.nl`' en als poort 119 (standaard). De overige instellingen kunt u laten zoals ze zijn.

1.12.5 Adreslijstservice ('directory')

Om personen te kunnen opzoeken, is er in kennisnet een zogenoemde LDAP-server geïnstalleerd. Deze machine bevat e-mailadressen van alle kennisnetgebruikers. Om deze machine te kunnen raadplegen, dient de machine te worden ingesteld voor gebruik.

Kies in het voorkeurenvenster de categorie 'E-mail & Groepen', sub 'Directory'.



Figuur 50: voorkeuren 'Directory'

Om kennisnet aan de lijst toe te voegen[4], klikt u op 'Nieuw...'. Er verschijnt een venster waarin u gegevens over de LDAP-server van kennisnet dient in te geven.



Figuur 51: eigenschappen nieuwe directory

Achter 'Beschrijving:' kunt u een willekeurige naam kiezen, maar 'kennisnet' is wellicht een goede suggestie. Het adres van de server is '`ldap.kennisnet.nl`'. Achter 'Zoekwortel:' kunt u enige restricties aangeven met betrekking tot het te doorzoeken domein. U kunt hier volstaan met de tekst '`c=nl`' ('country equals the Netherlands', ofwel: zoek alleen in Nederland). Achter het poortnummer kunt u het standaard poortnummer (389) ongemoeid laten. Klik op 'OK' om het venster te sluiten. Met de pijltjesknoppen kunt u de LDAP-server van kennisnet eventueel een hogere prioriteit geven door deze naar boven te verplaatsen.

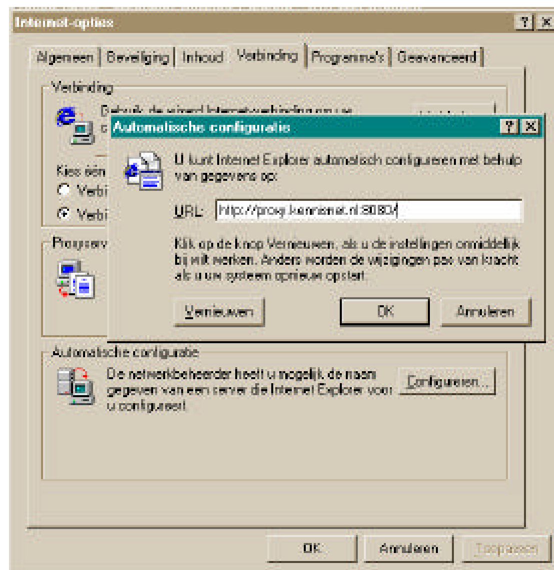
1.13 Wat moet ik instellen in Internet Explorer?

Er is een vrij sterk verschil tussen Internet Explorer 4 en Internet Explorer 5. Voor beide programma's volgt hier uitleg.

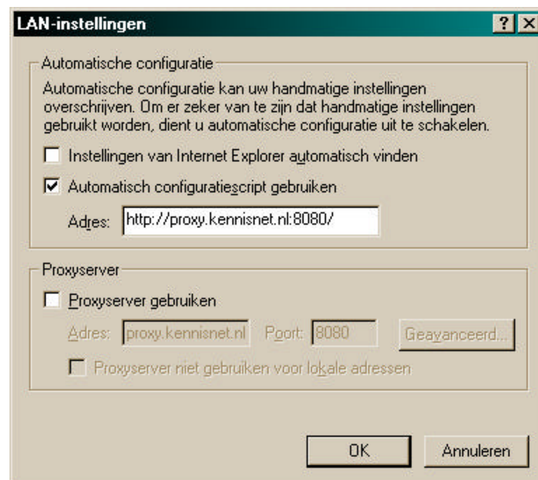
[4] Zeer waarschijnlijk zijn door de firewall-restricties de andere genoemde LDAP-servers niet bereikbaar vanaf kennisnet.

1.13.1 Internet Explorer 4

Open in Internet Explorer het menu 'Beeld' en vervolgens 'Internet-opties'. Ga dan naar het tabblad 'Verbinding'. Zie Figuur 52.



Figuur 52: Internet-opties: verbinding, MSIE 4.x



Figuur 53: Internet-opties: verbinding, MSIE 5.x

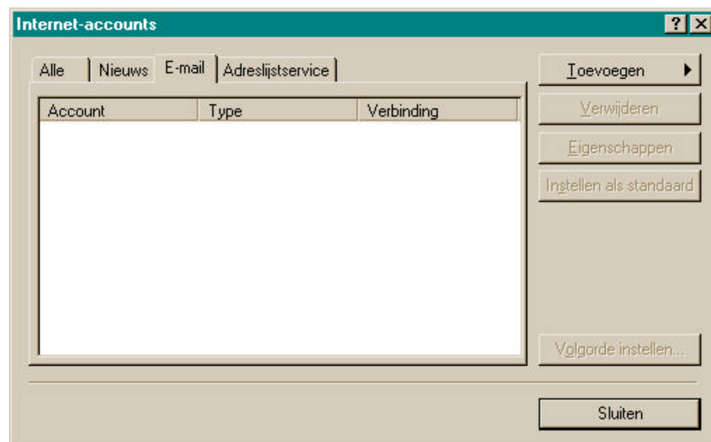
Om gebruik te maken van *automatische* proxy-instelling, dient de *handmatige* instelling te worden *uit*geschakeld. Klik vervolgens bij 'Automatische configuratie' op de knop 'Configureren'. Vul in het venster dat dan verschijnt, achter 'URL:' het adres van de proxyserver in: `http://proxy.kennisnet.nl:8080/`. Klik op 'OK' en nogmaals op 'OK' om het optievenster te sluiten.

1.13.2 Internet Explorer 5

Kies het menu 'Extra' en dan 'Internet-opties'. Ga naar het tabblad 'Verbinding' en klik op de knop 'LAN-instellingen...'. Er verschijnt een venster (zie Figuur 53). Gebruik de automatische configuratie. Schakel hiertoe de optie 'Automatisch configuratiescript gebruiken' in en vul achter 'Adres' in: `http://proxy.kennisnet.nl:8080/`. Zorg dat 'Proxyserver gebruiken' **niet** is ingeschakeld. Klik op 'OK' en nogmaals op 'OK' om het optievenster te sluiten.

1.14 Wat moet ik instellen in Outlook of Outlook Express?

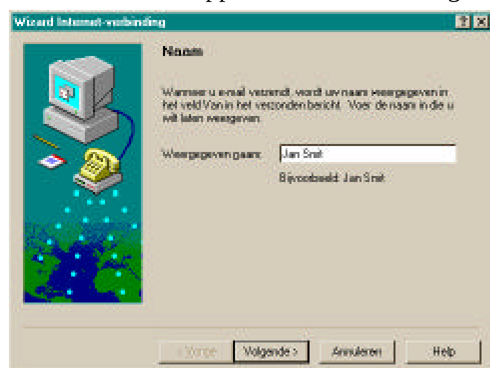
Start Outlook of Outlook Express. Kies het menu 'Extra' en vervolgens 'Accounts'. Er verschijnt een venster met een drietal (Outlook) of viertal (Outlook Express) tabbladen.



Figuur 54: Internet-accounts in Outlook (Express)

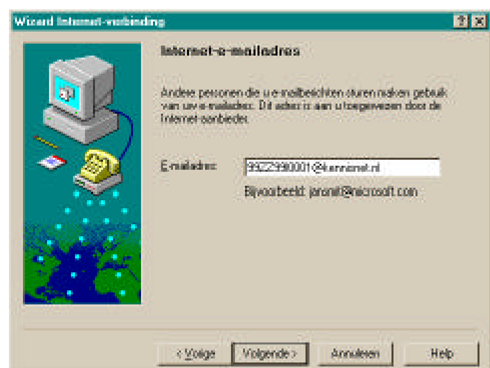
1.14.1 E-mail in Outlook (Express)

Selecteer het tabblad 'E-mail'. Klik op de knop 'Toevoegen' en selecteer 'E-mail…'. Vervolgens wordt u in een zevental stappen door een Wizard geleid om een e-mailaccount aan te maken.



1. In de eerste stap wordt uw (eigen, echte) naam gevraagd. Vul dit in en klik op 'Volgende>'.

Figuur 55: account-wizard: Naam



2. In de tweede stap dient u uw e-mailadres in te vullen.

Figuur 56: account-wizard: Internet-e-mailadres

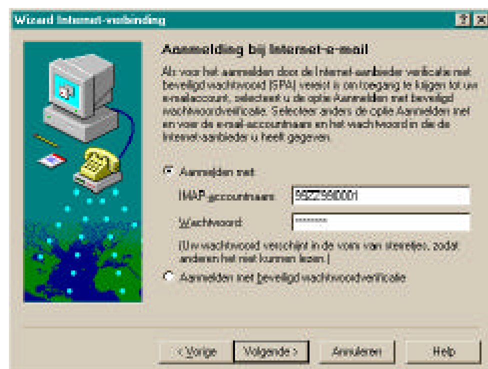


Figuur 57: account-wizard: E-mailservernamen

3. In de volgende stap dienen de mailservers voor inkomende en uitgaande mail te worden ingesteld. Bij de inkomende mail moet een keuze worden gemaakt uit IMAP4 of POP3.

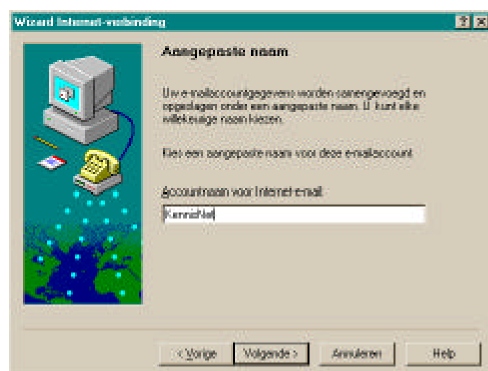
IMAP4 biedt, beter dan POP3, de mogelijkheid om berichten op de server achter te laten. POP3 is vooral bedoeld om berichten op de lokale computer op te slaan. Beide hebben voor- en nadelen. Zie deel VII (Veelvoorkomende vragen) en VIII (Begrippenlijst) voor een nadere toelichting over het verschil tussen POP3 en IMAP4.

Voor gebruik van IMAP4 is de server voor inkomende mail `imap.kennisnet.nl`, voor POP3 is dit `pop.kennisnet.nl`. De server voor uitgaande mail is in beide gevallen `smtp.kennisnet.nl`



Figuur 58: account-wizard: Aanmelding

4. In het volgende scherm wordt gevraagd om de gebruikersnaam (dus niet uw eigen naam in het dagelijks leven) en het bijbehorende wachtwoord. Aanmelden met beveiligd wachtwoordverificatie is niet nodig; dit wordt ook niet ondersteund.



Figuur 59: account-wizard: Aangepaste naam

5. Kies in de vijfde stap een korte omschrijving voor het e-mailaccount, bijvoorbeeld ‘kennisnet’.



Figuur 60: account-wizard: type verbinding

6. In de zesde stap moet gekozen worden voor het type verbinding. Dit dient als 'LAN-netwerk gebruiken' te worden ingesteld.

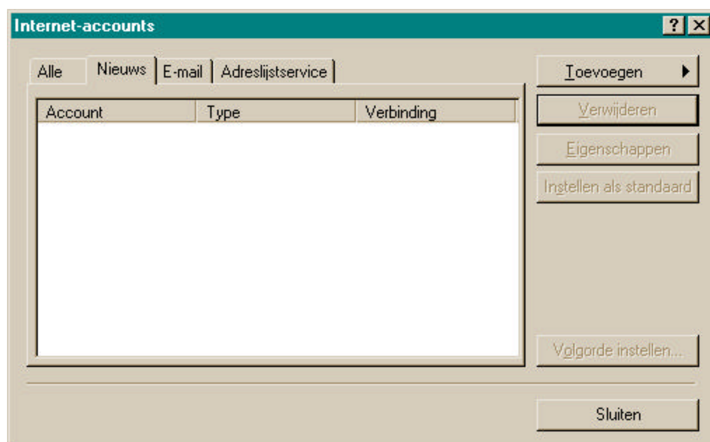


Figuur 61: account-wizard: Voltooien

7. De laatste stap is bedoeld als bevestiging. Klik op 'Voltooien' om de instelling af te ronden.

1.14.2 Discussiegroepen in Outlook Express

Om deel te kunnen nemen aan discussiegroepen, dient u in Outlook Express[5] de server waarvandaan u de berichten wilt ophalen en waarmee u uw berichten wilt plaatsen, in te stellen. Ga naar het tabblad 'Nieuws' in het accountvenster.



Figuur 62: Nieuws

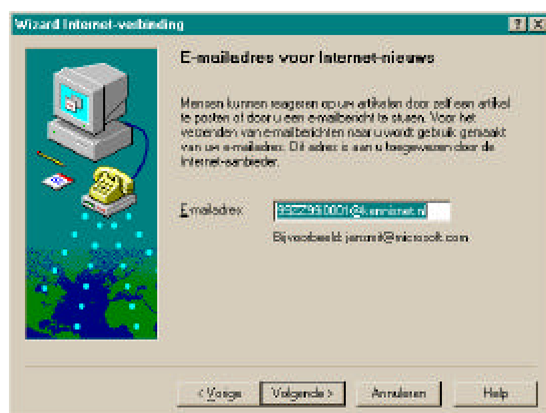
[5] Outlook zelf heeft geen ondersteuning voor discussiegroepen, maar gebruikt hiervoor Outlook Express.

Klik op 'Toevoegen' en selecteer 'Nieuws…'.



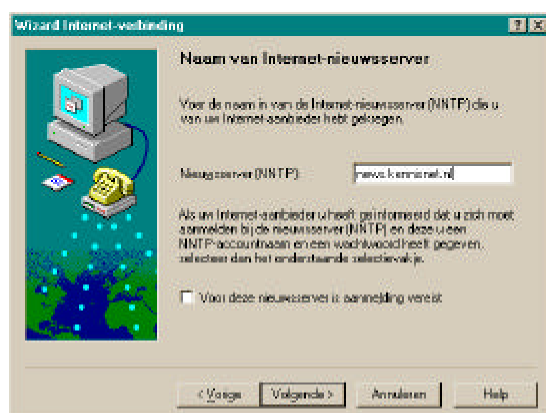
Figuur 63: account-wizard: Naam

In het eerste venster dat dan verschijnt, wordt u gevraagd om uw echte naam in te vullen. Typ uw naam en klik op 'Volgende>' om verder te gaan.



Figuur 64: account-wizard: E-mailadres

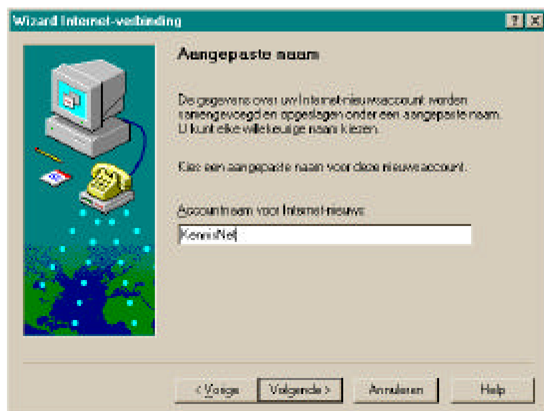
Vervolgens wordt u gevraagd om uw e-mailadres in te vullen. Typ het adres waarop u eventuele reacties op uw berichten wenst te ontvangen en klik op 'Volgende>' om verder te gaan.



Figuur 65: account-wizard: nieuwsserver

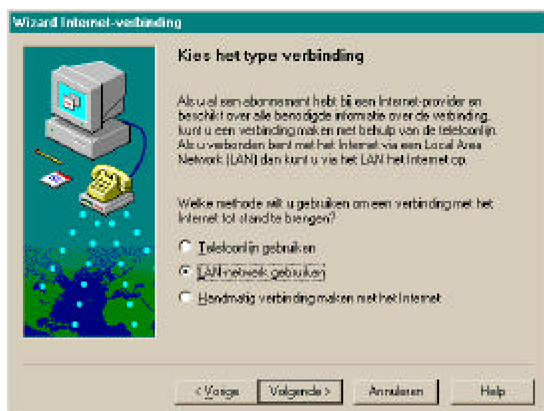
Het derde venster is bedoeld om het adres van de nieuwsserver op te geven. Het adres is in dit geval `news.kennisnet.nl`. U hoeft zich niet aan te melden aan de server.

Klik hierna op 'Volgende>'.



Figuur 66: account-wizard: Aangepaste naam

U kunt in het vierde venster een 'aangepaste naam', ofwel een korte omschrijving van de nieuwsserver opgeven. Een gepaste naam zou wellicht 'kennisnet' kunnen zijn. Klik daarna op 'Volgende>'.



Figuur 67: account-wizard: type verbinding

U wordt vervolgens gevraagd op welke wijze u een verbinding wenst te leggen met de zojuist ingevoerde nieuwsserver. Standaard staat dit op 'LAN-netwerk gebruiken', wat ook de keuze is die u dient aan te geven. Klik dus op 'Volgende>' om naar het laatste venster te gaan.

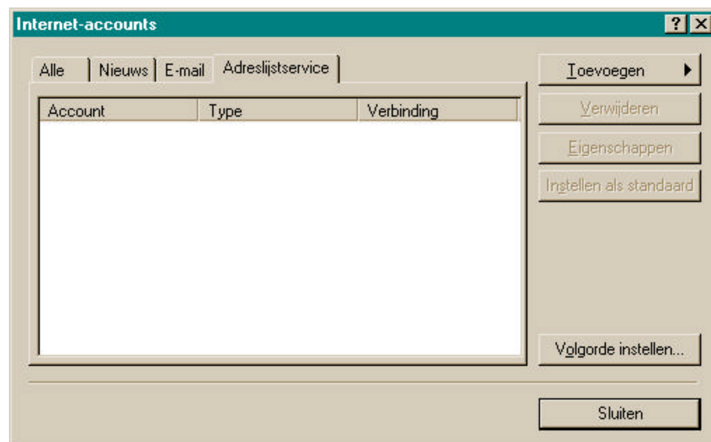


Figuur 68: account-wizard: voltooien

U kunt het invoeren van de nieuwsserver bevestigen door in het laatste venster op 'Voltooien' te klikken. Eventueel kunt u nog andere opties aanpassen door met de knop '<Vorige' één of enkele stappen terug te gaan.

1.14.3 Adreslijstservice in Outlook (Express)

Om personen te zoeken in kennisnet, kunt u gebruikmaken van de centrale 'LDAP-server'. Ga naar het tabblad 'Adreslijstservice' in het accountvenster.



Figuur 69: Adreslijstservice

Klik op 'Toevoegen' en kies 'Adreslijstservice'. Er komt, net zoals bij e-mail en nieuws, een wizard die u door het aanmaken van een nieuwe adreslijstservice leidt.



Figuur 70: account-wizard: LDAP-server

In het eerste venster wordt u gevraagd om het adres van de zogenoemde LDAP-server in te geven. Typ '`ldap.kennisnet.nl`' en klik op 'Volgende>'.

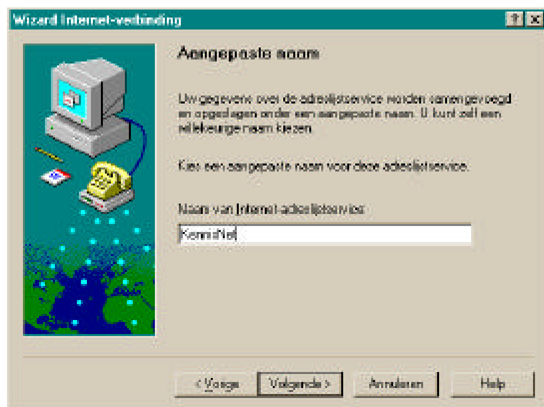


Figuur 71: account-wizard: E-mailadressen controleren

In het tweede venster wordt gevraagd of u de LDAP-server wilt gebruiken om e-mailadressen te controleren aan de hand van een naam. Als u bij het verzenden van een bericht een persoonsnaam intypt, controleert Outlook normaal uw adressenboek, maar indien u hier 'Ja' antwoordt, bovendien ook de LDAP-server op het voorkomen van de betreffende naam.

Het opzoeken van de naam in de LDAP-server kan vertragend werken, zoals is aangegeven in het venster. U kunt het beste 'Nee' antwoorden, indien u niet altijd een verbinding hebt met kennisnet.

Klik op 'Volgende' om verder te gaan.



Figuur 72: account-wizard: Aangepaste naam adreslijstservice

In het derde venster kunt u een 'aangepaste naam', ofwel een omschrijving geven van de adreslijstservice. Een handige keuze is wellicht 'kennisnet'.



Figuur 73: account-wizard: voltooien

In het laatste venster wordt u geacht om het geheel te voltooien. Klik op 'Voltooien' om het aanmaken van een adreslijstservice af te ronden.

1.15 Mijn bladerprogramma ondersteunt geen automatische proxyconfiguratie. Hoe kan ik toch surfen?

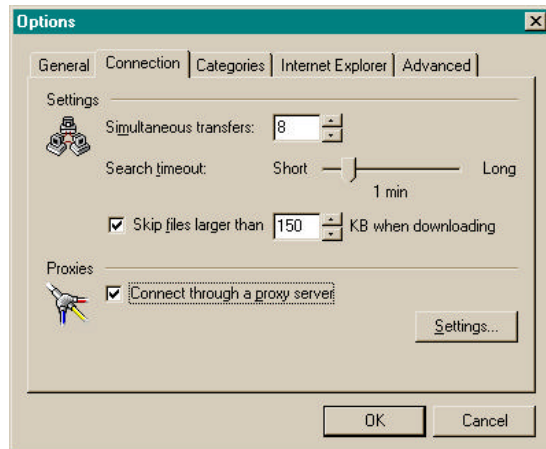
In dit geval moet u kiezen voor handmatige instelling van de proxyconfiguratie. De proxyserver heeft als adres '`proxy.kennisnet.nl`' en poortnummer 8080. Deze instelling kan worden gebruikt voor WWW (HTTP), beveiligd WWW (HTTPS), FTP en Gopher.

Indien uw bladerprogramma helemaal geen proxy configuratie ondersteunt, dient u een ander bladerprogramma te bemachtigen.

1.16 Kan ik Copernic gebruiken op kennisnet?

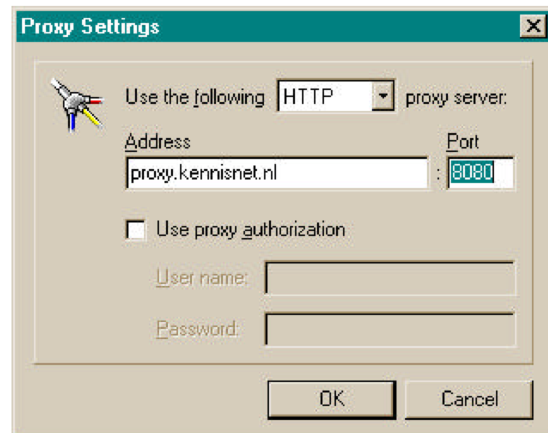
Copernic is een 'zoekagent'; met andere woorden: een programma dat tracht de kracht van een aantal zoekmachines op het Internet te combineren en diverse zoekmachines parallel te raadplegen. Inderdaad is het mogelijk om met Copernic ook via kennisnet informatie te zoeken op het Internet. Copernic werkt met hetzelfde protocol als uw bladerprogramma en dient daarom ook gebruik te maken van de proxyservers van kennisnet. U kunt dit als volgt instellen.

In het menu 'View' kiest u 'Options'. Er verschijnt een venster waarin u diverse opties kunt opgeven op verschillende tabbladen. Ga naar het tabblad 'Connection'.



Figuur 74: Copernic: verbindingsopties

Vink het vakje 'Connect through a proxy server' aan. Het knopje 'Settings...' wordt geactiveerd. Klik er nu op om de proxy in te stellen.



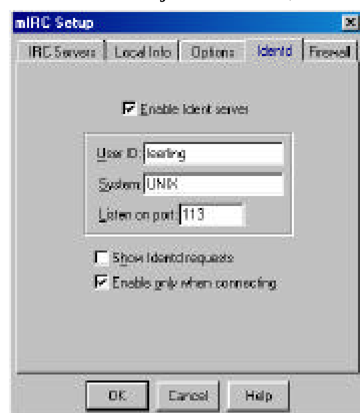
Figuur 75: Copernic: proxy-instellingen

In het keuzevakje staat standaard 'HTTP'. Dit dient u zo te laten. Onder 'Address' kunt u invullen '`proxy.kennisnet.nl`'. Onder 'Port' vult u het poortnummer, '`8080`' in. U hoeft zich *niet* bij de proxyservers aan te melden, dus 'Use proxy authorization' dient u *niet* aan te vinken.

Klik op 'OK' en nogmaals op 'OK' en u kunt aan de slag.

1.17 Wat moet ik instellen in mIRC?

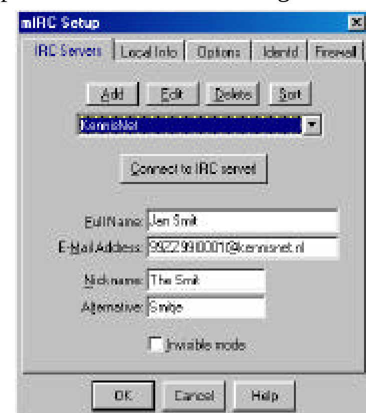
Een bekend programma voor IRC (Internet Relay Chat) is mIRC. Dit programma is geschikt om via een proxy met servers op het Internet te communiceren. Bij het opstarten toont het programma een venster met vijf tabbladen, waarvan er drie belangrijk zijn voor het opzetten van een verbinding.



Figuur 76: mIRC: Identd



Figuur 77: mIRC: Firewall



Figuur 78: mIRC: IRC Servers

Identd is een typische UNIX-service. Sommige IRC-servers stellen er prijs op dat de gebruikers zich via de 'identd' legitimeren. Mogelijk kan het nuttig zijn om dit in te schakelen. Geef een gebruikersnaam op. Zie Figuur 76.

Firewall. Om met servers buiten kennisnet te kunnen communiceren is het noodzakelijk dat ondersteuning voor de socks-proxy [6] wordt ingesteld. Op het tabblad 'Firewall' (Figuur 77) dient het vakje 'Use SOCKS firewall' aangevinkt te worden. Het te gebruiken protocol is Socks4 of Socks5. Vul als 'Hostname' in 'proxy.kennisnet.nl' en poort 1080. Er is geen user ID of wachtwoord nodig.

IRC Servers. Op het eerste tabblad kunnen servers worden ingesteld. Er is al een grote lijst met servers voorgeprogrammeerd, waaruit kan worden gekozen. Geef in ieder geval een eigen naam op, een e-mailadres en een 'Nickname' (pseudoniem). Eventueel kan een alternatief pseudoniem worden opgegeven.

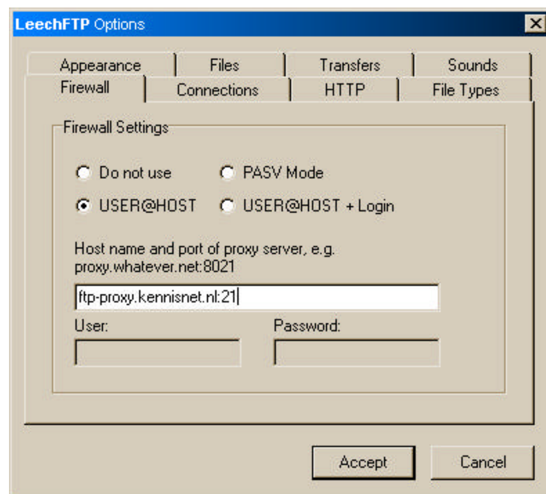
1.18 Hoe kan ik FTP'en via de proxy?

Voor het FTP-protocol wordt gebruikgemaakt van een speciale FTP-proxyservice op de eerste proxyserver. U dient, indien uw FTP-programma dit ondersteunt, het zo in te stellen, dat gebruik wordt gemaakt van de firewall volgens de methode 'USER@HOST'.

Hieronder wordt uitgelegd hoe een aantal FTP-programma's kan worden ingesteld.

Let op dat u alleen via de ftp-proxy kunt FTP'en. U kunt op deze manier uitsluitend naar FTP-services op poort 21 (de standaard FTP-poort) verbinden; indien het noodzakelijk is om naar een andere poort te verbinden, dient u gebruik te maken van de HTTP-proxy, bijvoorbeeld met Netscape Communicator of Internet Explorer.

[6] Zie ook deel I en deel VIII voor uitleg van het begrip 'proxy'. SOCKS is een bepaald protocol dat aan bepaalde andere op Internet gebruikte protocollen toegang biedt tot diensten die zich buiten het lokale netwerk en achter de firewall bevinden.



Figuur 79: LeechFTP

1.18.1 LeechFTP

Selecteer uit het menu 'File' de keuze 'Options…'. Kies in het venster dat dan verschijnt het tabblad 'Firewall'.

Selecteer de optie 'USER@HOST' en vul onder 'Host name and port…' in:

'ftp-`proxy.kennisnet.nl:21`'

Klik op 'Accept' om de instellingen te bewaren en het venster te sluiten.

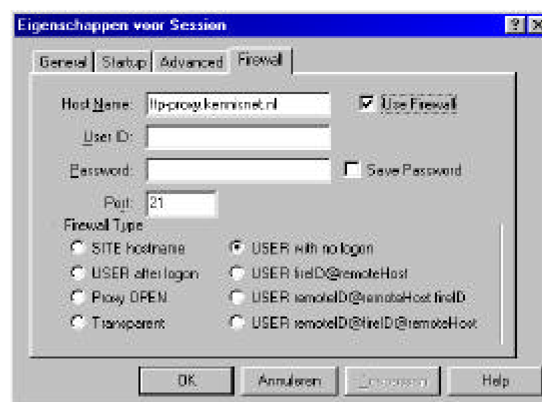
1.18.2 WS-FTP lite

Wanneer op de knop 'Connect' (Verbinden) wordt gedrukt, verschijnt een venster waarin alle gegevens voor de op te zetten verbinding kunnen worden ingegeven.

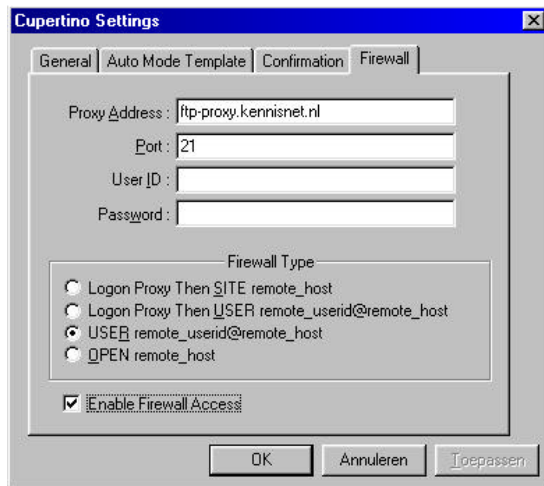
Selecteer het tabblad 'Firewall'. Geef als 'Host Name:' het adres '`ftp-proxy.kennisnet.nl`' en vul achter 'Port:' het getal `21` in. Kies het type 'USER with no logon' en activeer het gebruik van de firewall door het vakje 'Use Firewall' aan te vinken.

Klik op toepassen **['OK']** en vul op het tabblad 'General' de verdere gegevens voor de verbinding in (bestemming, gebruikersnaam op de andere machine, etc.).

Let op: u dient deze handeling voor iedere te bezoeken machine te herhalen!



Figuur 80: WS FTP lite edition



Figuur 81: Cupertino

1.18.3 Cupertino

Selecteer uit het menu 'Tools' de keuze 'Settings'. Ga in het venster dat verschijnt naar het tabblad 'Firewall'.

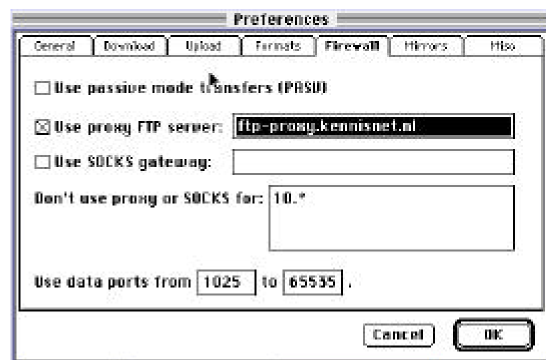
Vul achter 'Proxy Address:' het adres '`ftp-proxy.kennisnet.nl`' in en achter 'Port:' het getal 21. Laat de rest leeg. Kies als type firewall:

'USER remote_userid@remote_host'.

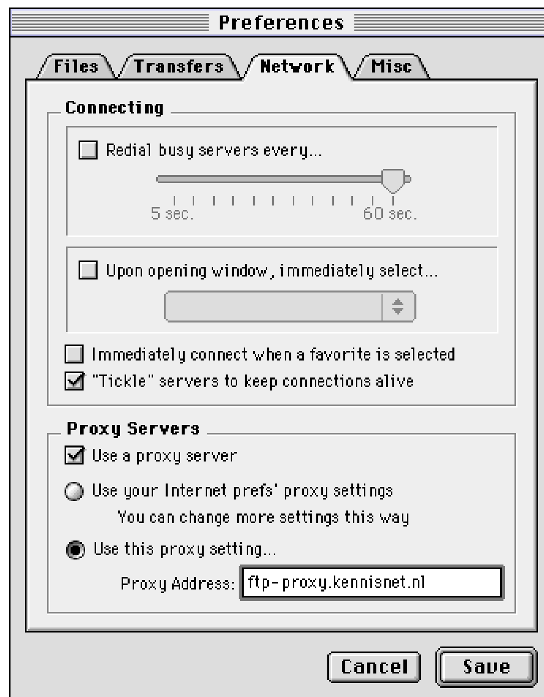
Bewaar de instelling door uit het menu 'Tools' de keuze 'Save settings now…' te selecteren.

1.18.4 Fetch (Macintosh)

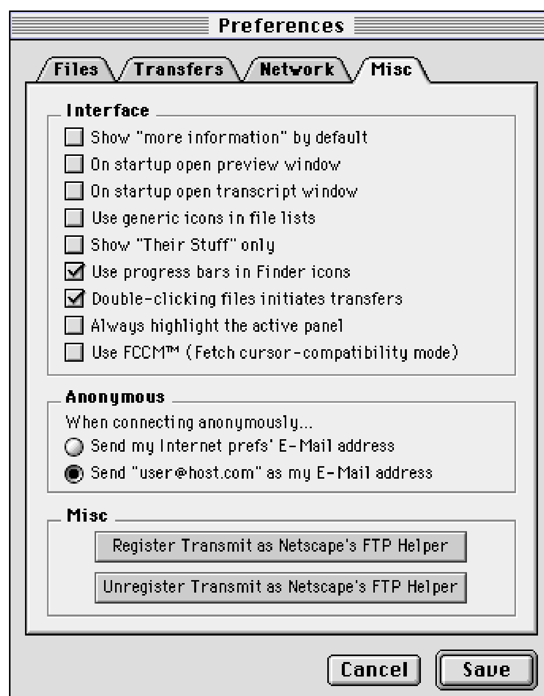
Kies uit het menu 'Customize' de optie 'Preferences'. Ga naar het tabblad 'Firewall' Selecteer 'Use proxy FTP server:' en typ daarachter '`ftp-proxy.kennisnet.nl`'.



Figuur 82: Fetch



Figuur 83: Transport/Transmit



Figuur 85: overige opties

1.18.5 Transport/Transmit (Macintosh)

Kies uit het menu 'Edit' de optie 'Preferences'. Ga in het venster naar het tabblad 'Network'. Vink het vakje 'Use a proxy server' aan en selecteer de optie 'Use this proxy setting…'. Vul dan achter 'Proxy Address:' het adres '`ftp-proxy.kennisnet.nl`' in. Klik op 'Save' om de opties te bewaren.

Transport/Transit kent overigens nog enkele opties die de moeite waard zijn om in te stellen. Op het eerste tabblad ('Files') is een vak met de titel 'Permissions'.



Figuur 84: Transport/Transmit: Permissions

U kunt hier aangeven welke rechten u standaard wilt geven aan een bestand dat u verstuurt. Dit is geënt op instellingen voor UNIX-servers, waarbij onderscheid wordt gemaakt in rechten (lezen – 'read'), schrijven ('write'), uitvoeren ('execute') voor de eigenaar, een groep en de rest van de wereld. In het geval van onderhoud van een webserver wilt u waarschijnlijk graag dat de rest van de wereld kan lezen, maar alleen uzelf en eventuele medeleden van uw groep de bestanden kunnen wijzigen.

In Figuur 85 is het vierde tabblad te zien. Hier zijn met name de opties 'Anonymous' en 'Misc' interessant. Bij de eerste kunt u aangeven welk e-mailadres wordt opgegeven bij 'anoniem' gebruik van FTP. In de eerste optie wordt uw e-mailadres gegeven; in het tweede geval een fantasieadres. Aangezien het meestal niet nodig is om een echt adres op te geven, heeft de laatste optie de voorkeur.

Onder 'Misc' kunt u, indien u Netscape Navigator of Communicator gebruikt, aangeven dat dit programma Transport/Transmit dient te gebruiken voor FTP in plaats van de ingebouwde functionaliteit. De tweede knop schakelt deze optie weer uit.

1.19 Kan ik ook zonder proxyinstellingen FTP'en?

Dat kan, mits uw FTP-programma er geen problemen mee heeft dat er een apenstaartje ('@') in de gebruikersnaam voorkomt en een voldoende lange gebruikersnaam accepteert, zodat daar ook het adres van de te benaderen machine in kan voorkomen.

De truc is vrij eenvoudig. U maakt via FTP een verbinding met de proxyserver (`ftp-proxy.kennisnet.nl`) op de standaard FTP-poort (21). U geeft geen gewone gebruikersnaam, maar de gebruikersnaam op de doelmachine, een apenstaartje en het adres van de doelmachine, bijvoorbeeld: `user@www.kennisnet.nl`. Vervolgens zal gevraagd worden om het wachtwoord voor de doelmachine, behorend bij de gebruikersnaam.

Hieronder volgt een voorbeeld van een sessie in een DOS-venster onder Windows 98.

```
FTP
Auto
C:\WINDOWS>ftp ftp-proxy
Verbonden met ftp-proxy.kennisnet.nl.
220-you are using the ftp proxy to www.kennisnet.nl
220 please supply : <userid>@www as name
Gebruiker (proxy.kennisnet.nl:(none)): demo@10.17.42.105
331-(----GATEWAY CONNECTED TO 10.17.42.105----)
331-(220 educatiefnet.kennisnet.nl FTP server (Version wu-2.4.2-academ[BETA-15](
1) Wed May 20 13:45:04 CDT 1998) ready.)
331 Password required for demo.
Wachtwoord:
230 User demo logged in.
ftp>
```

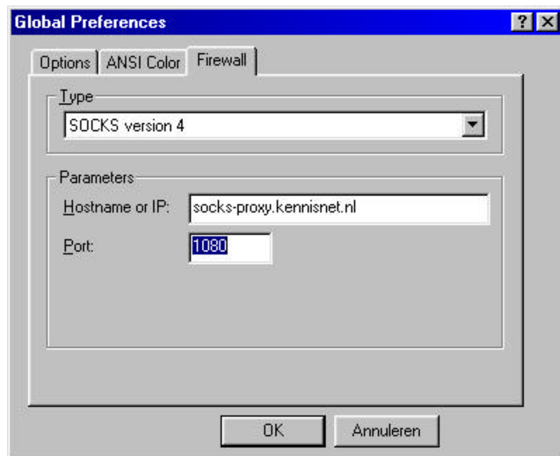
Figuur 86: FTP-sessie via DOS

1.20 Kan ik ook telnetten naar het Internet?

Ja, dat kan, mits u een 'SOCKSified' telnetprogramma hebt. Hieronder wordt een aantal van dergelijke telnetprogramma's besproken. Een andere 'truc', echter alleen voor Windows, is om gebruik te maken van SocksCap, een stukje programmatuur dat het IP-netwerkverkeer opvangt, voorzover het via de firewall zou moeten lopen, en omleidt. Zie paragraaf 1.20.3.

1.20.1 CRT (Windows)

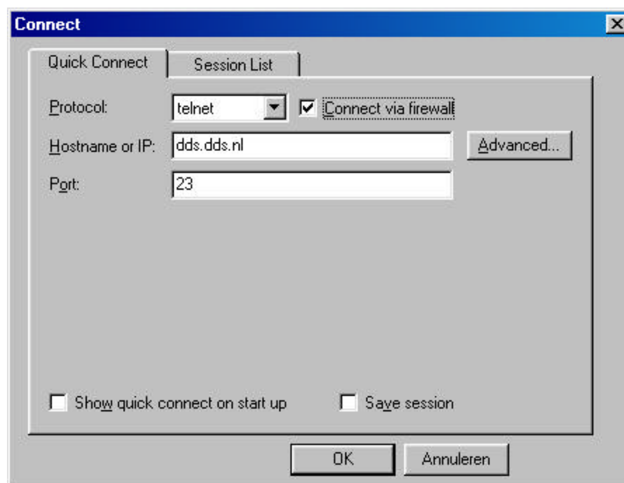
Eén van de telnetprogramma's die SOCKS ondersteunt, is CRT. Om het programma in te stellen voor het gebruik van de firewall, moet u de 'Global Preferences' aanpassen. Kies uit het menu 'Options' de keuze 'Global Preferences'. Het volgende venster verschijnt.



Figuur 87: CRT: Global Preferences

Ga naar het tabblad 'Firewall'. Selecteer onder 'Type' het type 'SOCKS version 4' of 'SOCKS version 5 (no authentication)'. Achter 'Hostname or IP:' dient u '`socks-proxy.kennisnet.nl`' te typen en achter 'Port:' het poortnummer: `1080`.

Wanneer u een verbinding wilt opzetten, dient u expliciet aan te geven dat u gebruik wilt maken van de SOCKS-firewall. Hieronder ziet u het scherm waarmee u de instellingen voor een verbinding kunt ingeven.



Figuur 88: CRT: Connect

Op het tabblad 'Quick Connect' vinkt u 'Connect via firewall' aan. Vul vervolgens het adres van de machine en het poortnummer in, waar naartoe u wilt telnetten. Klik op 'OK' en de verbinding wordt opgezet.

1.20.2 Mocha Telnet (Java)

De Java-versie van Mocha Telnet (`http://www.mochasoft.dk/java.html#telnet`[7]) ondersteunt SOCKS4. Om gebruik te maken van de SOCKS-proxy van kennisnet, dient u het bestand '`telnet2.html`' dat bij het pakket zit, te wijzigen, d.w.z. enkele parameters voor het Java-applet toe te voegen. Hieronder is de code voor het HTML-bestand gegeven.

[7] Op dit adres kunt u een demonstratieversie ophalen; voor het volledige programma dient u te betalen.

```
<HTML>
<HEAD>
<TITLE> Mocha Telnet </TITLE>
</HEAD>
<BODY>
<APPLET CODE="telnet.class" WIDTH=1 HEIGHT=1>
<param name=type value="frame">
<param name=screen_x value="100">
<param name=screen_y value="100">
<param name=screen_width value=600>
<param name=screen_height value=500>
<param name=proxy_host value="socks-proxy.kennisnet.nl">
<param name=proxy_port value=1080>
<param name=proxy_socks value=true>
</APPLET>
</BODY>
</HTML>
```

Tabel 1: HTML-code voor proxyconfiguratie

Omdat het een Java-applet betreft, kan het programma in principe op ieder type computer werken, waarvoor Java wordt ondersteund. Indien uw bladerprogramma de mogelijkheid biedt om netwerkbeveiligingen (tijdelijk) uit te schakelen voor Java, kunt u het programma starten door met uw bladerprogramma het bovenstaande HTML-bestand te openen.

Een andere optie is om de 'appletviewer' van de Java Development Kit of de Java Runtime Environment te gebruiken[8].

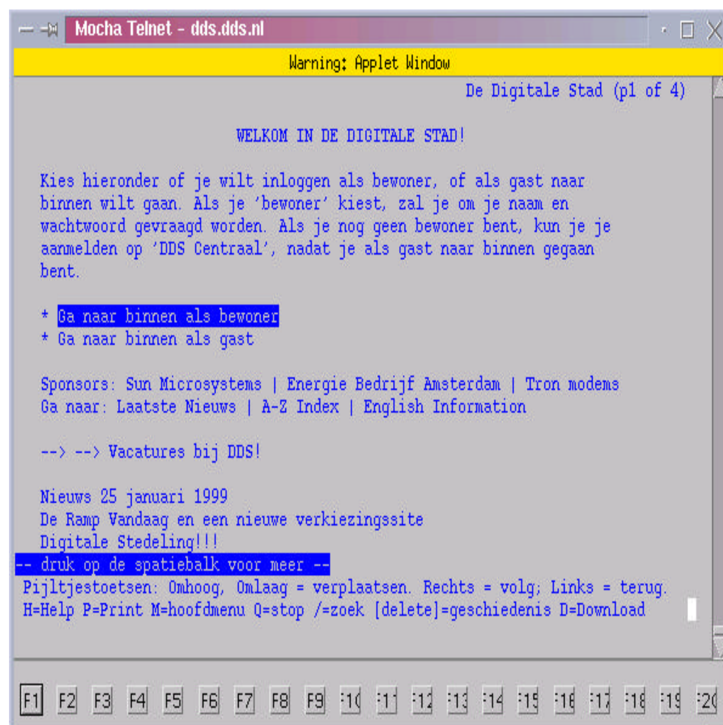
In Figuur 89 is een voorbeeld getoond van Mocha Telnet, uitgevoerd door de 'appletviewer' onder Linux. Ditzelfde kunt u ook onder Windows of op een Macintosh. Voor Windows kunt u een kort 'batch'-bestand (script) maken, dat met de appletviewer het telnetprogramma start. Noem dit bestand bijvoorbeeld 'MTELNET.BAT'. U kunt eenvoudig een icoontje maken om het programma te starten.

```
%ECHO OFF
APPLETVIEWER telnet2.html
```

Tabel 2: MTELNET.BAT

Informatie over het starten van Java-applets onder MacOS kunt u vinden op het adres http://developer.apple.com/techpubs/java/MacOSandJava/JManager/JManager2.1/JManager.21.html.

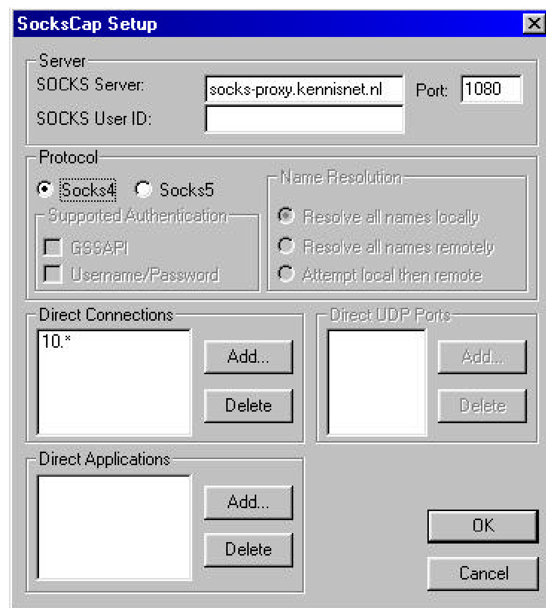
[8] De Java Development Kit of Java Runtime Environment kunt u ophalen bij JavaSoft: http://www.javasoft.com/products/index.html. Kies het voor u geschikte platform, eventueel kunt u kijken bij 'ports' voor *uw* besturingssysteem.



Figuur 89: Mocha Telnet voor Java tm

1.20.3 SocksCap

Met SocksCap (Windows) kunt u individuele programma's door een 'SOCKS'-firewall loodsen, wanneer zij gebruikmaken van protocollen die door SOCKS worden ondersteund. Telnet van Windows en TeraTerm werken hier in ieder geval mee samen. U kunt SocksCap ophalen van de website http://www.socks.nec.com/. U kunt kiezen uit een versie voor Window 3.x (16 bit) en Windows 95/98/NT (32 bit).



Figuur 90: SocksCap Setup

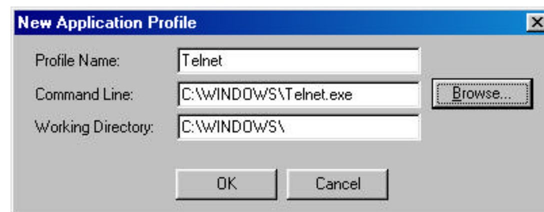
Kies uit het menu 'File' de optie 'Setup'. Er verschijnt een venster zoals getoond in Figuur 90. Achter 'SOCKS Server:' vult u in '`socks-proxy.kennisnet.nl`' en bij 'Port:' geeft u het getal 1080. 'SOCKS User ID:' kunt u leeg maken.

Kies als protocol 'Socks5'. Onder 'Name Resolution' kiest u 'Resolve all names locally'. Bij 'Direct Connections' klikt u op 'Add...'. In het venster dat dan verschijnt, vult u '`10.*`' in.

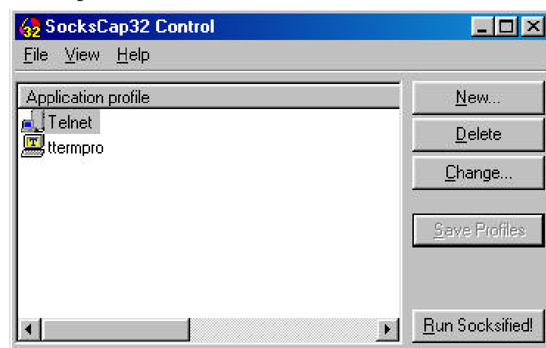
Klik op 'OK' om het venster te sluiten.

Vervolgens dient u applicaties in te stellen voor het gebruik van SocksCap. Als voorbeeld is in Figuur 91 de instelling voor Telnet.exe, welk standaard bij Windows 95/98/NT wordt geleverd. Met de 'Browse...'-knop zoekt u het programma, dat u via SOCKS wilt gebruiken, op. De meeste dingen worden direct ingevuld, eventueel kunt u de titel ('Profile Name:') nog aanpassen.

Klik op 'OK' om het venster te sluiten.



Figuur 91: SocksCap: instelling voor Telnet.exe



Figuur 92: SocksCap -hoofdvenster

U komt terug in het hoofdvenster. Klik op de knop 'Save Profiles' om de instellingen te bewaren.

Daarmee bent u klaar om te werken. Om een programma met SocksCap te starten, klikt u op de knop 'Run Socksified'. Hierdoor zal SocksCap een aantal systeemfuncties omleiden en uw programma zal, waar mogelijk, via de SOCKS-firewall naar het Internet worden geleid.

LET OP: SocksCap werkt niet voor alle TCP/IP-programmatuur; dit om u geen onnodige hoop te geven.

1.21 Kan ik ook RealAudio of RealVideo gebruiken?

Ja. Maar het probleem is, dat er in het verleden diverse verschillende protocollen zijn gebruikt voor het transporteren van 'Real' data. Niet voor alle protocollen zijn er mogelijkheden om deze op een nette manier door een firewall heen te transporteren. Vanaf de versie 'G2' van de RealPlayer is het mogelijk om gebruik te maken van het 'RTSP', 'Real-Time Streaming Protocol'. Een voorwaarde is echter weer, dat ook de server die de uitzending moet verzorgen, dit protocol ondersteunt. Voor dit protocol is een proxy-voorziening getroffen op `rtsp-proxy`, poort 554.

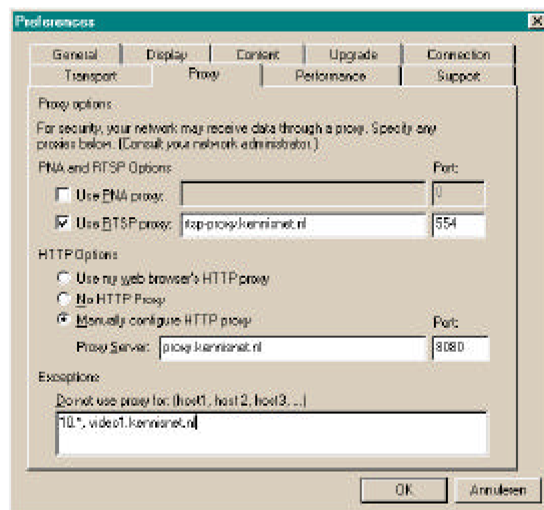
Een andere optie is het gebruik van HTTP, het protocol dat ook wordt gebruikt voor het versturen van webpagina's tussen webservers en bladerprogramma's. Dit protocol is echter niet ontworpen voor het communiceren van 'streaming data' (een voortdurende stroom gegevens) en servers zitten snel aan hun maximale capaciteit qua aantallen verbindingen.

Om de instellingen in de RealPlayer G2 te kunnen aanpassen voor kennisnet, kunt u in het programma zelf de optie 'Preferences' uit het menu 'Options' kiezen. Hiervoor dient het venster 'groot' te zijn, anders is het menu niet compleet. U kunt venster 'groot' maken door op de knop helemaal rechts te klikken.

Een andere manier is om in het configuratiescherm van Windows de instellingen voor RealPlayer G2 te selecteren.



Figuur 93: RealPlayer klein



Figuur 94: Proxyinstellingen G2

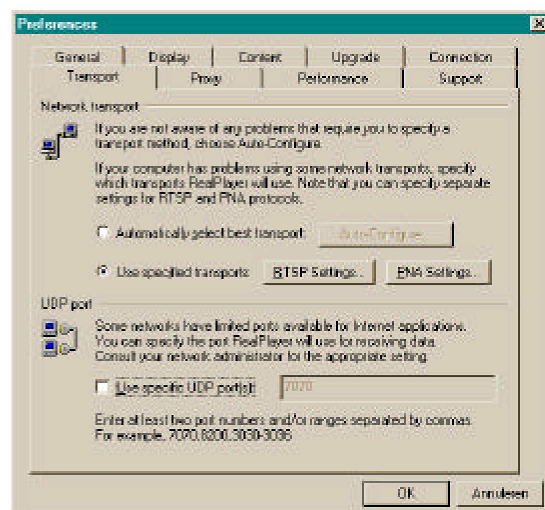
Ga naar het tabblad 'Proxy'. Laat de PNA-proxy uit staan, maar schakel de RTSP-proxy in. Vul als machinenaam '`rtsp-proxy.kennisnet.nl`' in en als poort dient u '`554`' aan te geven.

Onder ‘HTTP Options’ kunt u aangeven 'Use my web browser's HTTP proxy' om dezelfde proxy als uw bladerprogramma te gebruiken. Mogelijk is het beter om de instellingen met de hand in te geven. De proxyserver dient `proxy.kennisnet.nl`' (**let op:** dus zonder nummer!) te zijn en de poort '`8080`'.

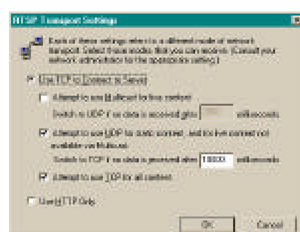
Onder 'Exceptions' kunt u aangeven welke adressen *niet* via de proxy moeten gaan. U dient hier in te vullen '`10.*, 127.*`'.

Op het tabblad 'Transport' kunt u de manier waarop bij voorkeur gegevens worden overgedragen, aangeven. Standaard zal het programma, zo mogelijk automatisch, proberen om de beste manier van gegevenstransport te selecteren. Helaas slaagt het programma er niet altijd in. In dat geval zult u het met de hand moeten instellen. Selecteer daarom de optie 'Use specified transports:'.

Met de knoppen 'RTSP Settings…' en 'PNA Settings...' kunnen de instellingen voor verschillende protocollen worden aangegeven.

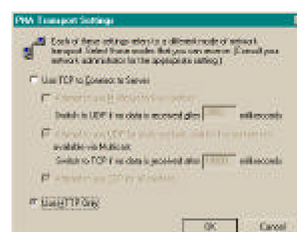


Figuur 95: transportinstellingen G2



Bij RTSP dient u 'Use TCP to Connect to Server' te selecteren. De eerste suboptie kunt u het beste **niet** selecteren, de beide andere wel.

Figuur 96: RTSP



Bij PNA dient u te kiezen voor 'Use HTTP Only'.

Figuur 97: PNA

1.22 Hoe kan ik de Windows Media Player gebruiken?

Om met de Windows Media Player (welke overigens ook voor MacOS beschikbaar is) media te kunnen afspelen, dient u uitsluitend van HTTP gebruik te maken. Het Microsoft-specifieke protocol voor de Media Player wordt *niet* ondersteund door de proxies van kennisnet.

Kies uit het menu 'Beeld' en dan 'Opties'. Er verschijnt een venster. Kies het tabblad 'Geavanceerd'. Op dit tabblad staat een lijstje met ondersteunde mediatypen. Selecteer 'Streaming Media (Windows Media)' en klik op ‘Wijzigen...’.

Figuur 99: opties Streaming Media

Geef 'proxy.kennisnet.nl' op als naam en poort 8080. Klik op 'OK'. Sluit het venster met 'Toepassen' en 'OK' en sluit het optievenster.

Figuur 98: Geavanceerde opties

In het venster (Figuur 99) dat dan verschijnt, dient u onder 'Protocollen' alle protocollen behalve HTTP uit te schakelen. Selecteer bij HTTP hetzij de optie 'Proxy-instellingen van de browser gebruiken', hetzij 'Gebruik proxy'.

In het laatste geval dient u het adres van de proxy in te stellen. Klik op 'Proxy-instelling configureren'.

Figuur 100: Media Player Proxy

1.23 Hoe kan ik de klok van de computers automatisch goed zetten?

Kennisnet heeft zogenoemde tijdservers, die u kunt gebruiken om de systeemklok van uw computers te synchroniseren. Deze tijdservers zijn te bereiken als `time.kennisnet.nl` en kunnen via het SNTP-protocol (Simple Network Time Protocol) benaderd worden. Er bestaan diverse hulpprogrammaatjes – commercieel, shareware en gratis – die u kunt gebruiken om de systeemklokken goed te zetten en bijvoorbeeld bij het opstarten van uw computer in de achtergrond te starten.

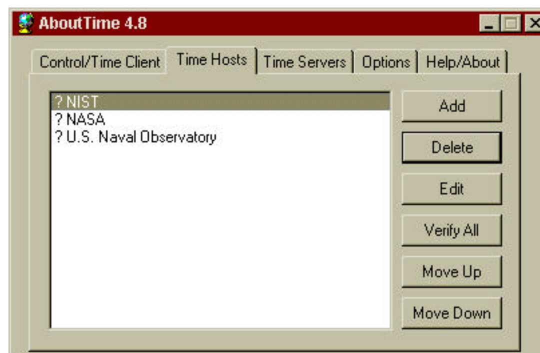
Echter, wanneer iedereen op kennisnet gebruik gaat maken van dezelfde tijdservers, zal dit ernstige gevolgen hebben voor de prestaties van deze machines. Het wordt daarom aangeraden om lokaal een eigen tijdserver op te zetten en die periodiek (bijvoorbeeld eens per dag) te laten synchroniseren met de centrale tijdservers. U kunt bijvoorbeeld op uw lokale netwerkserver een extra proces starten.

1.23.1 AboutTime

AboutTime is een klein, doch handig programmaatje voor het gelijkzetten van de tijd van lokale PC's. Het kan zowel client als server zijn. Hier volgt enige uitleg van de bediening van AboutTime op kennisnet.

Wanneer u AboutTime voor de eerste keer opstart, dient u nog enkele instellingen aan te passen voor de situatie op kennisnet. De standaard ingestelde servers zijn namelijk niet rechtstreeks bereikbaar op kennisnet.

Ga naar het tabblad 'Time Hosts'. Hier staan reeds drie timeservers aangegeven. Verwijder deze servers met de knop 'Delete'.



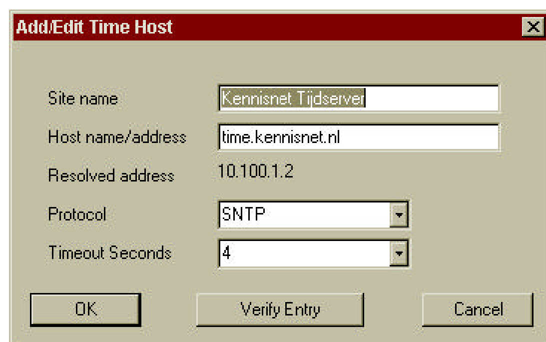
Figuur 101: AboutTime, Time Hosts

Vervolgens dient u de servers van kennisnet eraan toe te voegen. Klik op 'Add' om de opties voor de timeservers in te vullen.

Geef een omschrijving van de timeserver achter 'Site name', bijvoorbeeld 'kennisnet Tijdserver'. Achter 'Host name/address' dient u het adres van de timeserver in te vullen. Dit is:

- `time.kennisnet.nl`.

Het ‘Protocol’ dient te worden ingesteld op 'SNTP' (standaard) met een timeout van 4 seconden (standaard).



Figuur 102: AboutTime: toevoegen timeservers

Met de knop 'Verify Entry' kunt u controleren of de host bestaat. Deze knop stelt u *niet* in staat om de dienst zelf te testen.

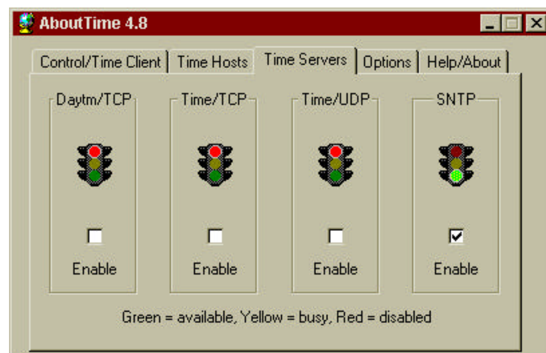
Indien de host niet bestaat of niet gevonden kan worden, krijgt u een foutmelding. Oorzaken kunnen zijn:

- DNS-probleem;
- geen verbinding;
- time-out.



Figuur 103: AboutTime, Oeps!

Wanneer u uw lijst van timeservers hebt ingevoerd, kunt u eventueel nog de volgorde bepalen met de knoppen 'Move up' en 'Move down'.

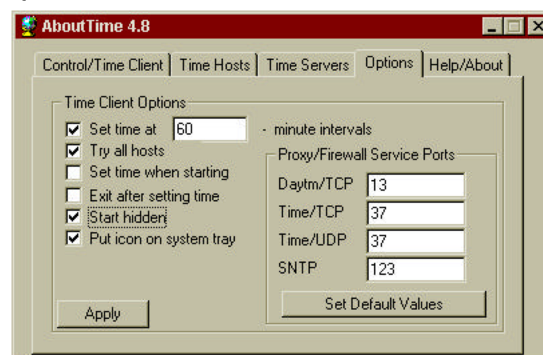


Figuur 104: AboutTime: Time Servers

Zoals gezegd kan AboutTime ook als server optreden. Ga voor de instellingen hiervoor naar het tabblad 'Time Servers'. Hier staat een viertal verkeerslichtjes met een aanvinkvakje eronder.

Door een vakje aan te vinken, zet u het verkeerslicht op groen en wordt de bijbehorende service actief. Elk van de verkeerlichtjes vertegenwoordigt een protocol om de tijd uit te wisselen. Standaard staan alle protocollen aan.

Het verdient aanbeveling om slechts één of twee machines in uw lokale netwerk aan de centrale server te laten refereren. De rest van de computers kan gebruikmaken van uw lokale systemen.



Figuur 105: AboutTime: Options

Ga tenslotte naar het tabblad 'Options'. Hier kunt u een aantal resterende instellingen invullen. Het kan nuttig zijn om de optie 'Start hidden' aan te vinken; hiermee wordt het programma onzichtbaar gestart. Door de optie 'Put icon on system tray' ook aan te vinken (standaard), is het icoontje wel zichtbaar in de systeembalk, normaliter rechts onder in het beeld.

Het interval tussen het verversen van de tijd ('Set time at') staat standaard ingesteld op 60 minuten. Deze tijd kunt u voor een lokale server gerust op een dag (= 60 maal 24 = 1440 minuten) instellen.

Met name voor lokale werkstations kan de optie 'Set time when starting' zinvol zijn om de tijd direct gelijk te zetten bij het opstarten van de PC of de sessie.

Op het eerste tabblad kunt u met de knop 'Hide' vervolgens het venster verbergen. Om 'AboutTime' altijd bij het aanmelden op het systeem te starten, kunt u een snelkoppeling in de groep 'Opstarten' van het Startmenu plaatsen.

1.24 Waar kan ik al die software krijgen of kopen?

Veel van de genoemde software is zonder problemen op het Internet te vinden. De genoemde bladerprogramma's zijn vrij verkrijgbaar via de producenten van de software. Zo kunt u de nieuwste versie van MS Internet Explorer vinden op de website van Microsoft: http://www.microsoft.com/. Netscape Communicator kunt u vinden op de website van Netscape Communications: http://home.netscape.com/, maar ook op vele andere websites en FTP-sites.

De genoemde FTP-software is vrijwel allemaal op te halen van 'Tucows': http://tucows.a2000.nl/ of http://www.tucows.com/. Kies in het hoofdmenu het gewenste software- en hardwareplatform en zoek de gewenste programmatuur. Andere bekende bronnen van software zijn http://www.download.com/ en http://www.software.com/. AboutTime kunt u verkrijgen op http://www.arachnoid.com/.

Let op dat deze software niet allemaal gratis is! Bepaalde producten kunt u maar voor een beperkte periode uitproberen, voordat u betaalt. Andere software heeft enkele functionaliteiten die pas worden ingeschakeld als u zich hebt geregistreerd en voor de software hebt betaald. Ook bij producten die als 'freeware' (gratis software) worden aangeboden, kan er een 'addertje onder het gras' zitten, bijvoorbeeld omdat de software slechts onder bepaalde omstandigheden of voor een beperkte doelgroep gratis is: meestal thuisgebruikers of educatieve instellingen. Ook mag u gratis software niet altijd verder verspreiden. **Lees dus altijd de licentievoorwaarden voordat u de software gaat gebruiken!**

Let op dat het Internet een vrij onveilig medium is als het gaat om softwaredistributie. Wees zeer zorgvuldig in het gebruik van software die van het Internet afkomstig is, zeker als het om onbekende websites of FTP-sites gaat. Controleer uw software vóór gebruik op mogelijke virusinfecties.

1.25 Hoe kan ik thuis gebruikmaken van kennisnetdiensten?

Uiteraard dient u in dit geval een verbinding te hebben met Internet via een andere Internetaanbieder. Raadpleeg deze voor alle informatie over hoe u verbinding dient te maken met het Internet en hoe u via deze aanbieder kunt 'surfen'. De diensten van kennisnet die u *buiten* kennisnet kunt gebruiken, zijn voornamelijk het lezen van uw elektronische post (e-mail) en in beperkte mate het raadplegen van informatie op kennisnet.

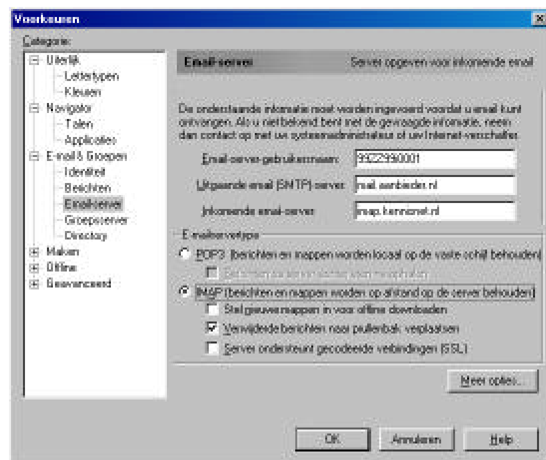
1.25.1 Thuis e-mail lezen en versturen

Om thuis uw e-mail te lezen, dient u dezelfde instellingen te gebruiken als op kennisnet zelf, **behalve** voor uw uitgaande post. Om te voorkomen dat er misbruik wordt gemaakt van de mailvoorzieningen van kennisnet, zijn er speciale filters aangebracht. Deze hebben echter ook tot gevolg dat u niet van buiten kennisnet post naar buiten kennisnet kunt verzenden. U dient daarom aan uw lokale Internetaanbieder te vragen via welke machine u uw e-mail kunt verzenden.

Hieronder volgen uitgewerkte voorbeelden voor Netscape Communicator en Outlook (Express). Hierbij wordt uitgegaan van de instellingen voor 'normaal' gebruik op kennisnet. In het voorbeeld wordt een denkbeeldige Internetaanbieder 'Aanbieder' gebruikt. Dit bedrijf heeft als server voor de uitgaande e-mailberichten een machine met de naam '`mail.aanbieder.nl`'. De exacte gegevens voor uw situatie moet u uiteraard navragen bij *uw* aanbieder.

In het geval u problemen ondervindt, zou u als uw *afzender*adres (het '`From:`'-veld in uw e-mail) het e-mailadres dat u van uw lokale aanbieder hebt gekregen, kunnen gebruiken, en als *antwoord*adres (het '`Reply-To:`'-veld in uw e-mail) uw kennisnetadres in kunnen vullen. In principe is dit vrijwel nooit nodig, maar sommige aanbieders controleren de informatie in berichtkoppen van uitgaande e-mailberichten op het '`From:’`-veld of dit binnen een door de aanbieder geaccepteerd domein valt. Een dergelijke controle wordt gedaan om 'SPAM' van binnenuit te voorkomen. U kunt hier meer over lezen in deel VII (Veelvoorkomende vragen).

Netscape



Figuur 106: instellingen Netscape om thuis mail te lezen en te versturen

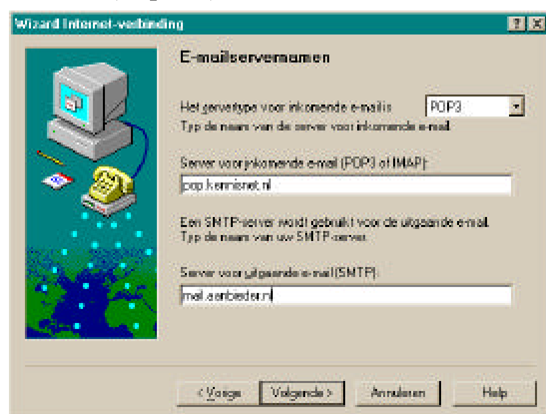
In Netscape Communicator stelt u de gegevens als volgt in. U kunt vrijwel alle instellingen overnemen uit de beschrijving in paragraaf 1.12.3.

Selecteer de categorie 'E-mail & Groepen' en vervolgens sub 'Email-server'.

U dient hier uw gebruikersnaam in te vullen voor kennisnet. Voor de uitgaande mail vult u het adres van de mailserver van uw lokale Internetaanbieder in; in dit voorbeeld '`mail.aanbieder.nl`'. Voor de inkomende mail geeft u, afhankelijk van uw keuze voor POP3 of IMAP4, het adres '`pop.kennisnet.nl`', respectievelijk '`imap.kennisnet.nl`' op.

Onder subcategorie 'Identiteit' kunt u, indien nodig, het antwoordadres instellen.

Outlook (Express)



Figuur 107: instellingen Outlook (Express) om thuis mail te lezen en te versturen.

Tijdens het aanmaken van een e-mailaccount via de account-wizard krijgt u, zoals ook in paragraaf 1.14.1 beschreven, een venster waarin u de mailserver opgeeft.

Als server voor inkomende mail geeft u, afhankelijk van uw keuze voor het POP3-protocol of het IMAP4-protocol, de naam '`pop.kennisnet.nl`' respectievelijk '`imap.kennisnet.nl`'.

Voor uitgaande mail gebruikt u de server van uw aanbieder; in dit voorbeeld '`mail.aanbieder.nl`'.

1.25.2 Thuis informatie van kennisnet raadplegen

Met uw bladerprogramma kunt uw altijd de externe webserver (`http://www.kennisnet.nl/`) benaderen. Het is echter mogelijk dat bepaalde pagina's zijn afgeschermd voor gebruik buiten kennisnet. De *interne* webserver (`http://web.kennisnet.nl/`) kunt u echter alleen binnen kennisnet benaderen.

1.26 Handige software

Om eenvoudig bruikbare netwerkinformatie op te zoeken, zijn er wat handige hulpmiddelen beschikbaar op het Internet. Deze hulpmiddelen voor MacOS en Windows zijn veelal een grafische afspiegeling van de UNIX-equivalenten welke vanaf de commandoregel aangeroepen kunnen worden.

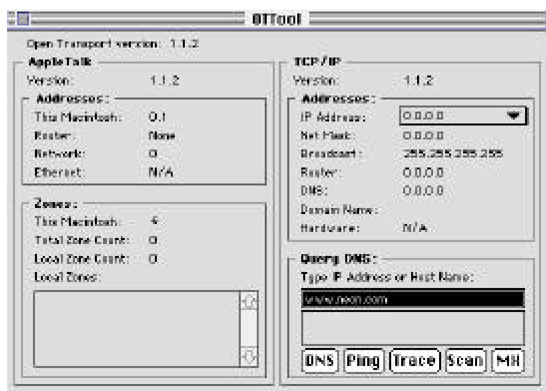
Let op dat dit soort software alleen bedoeld is om problemen mee op te lossen of te traceren en om informatie te bemachtigen. Het is zeker *niet* als 'speelgoed' bedoeld.

1.26.1 OTTool

De *gratis* OTTool voor MacOS is een stukje software dat informatie geeft over TCP/IP en AppleTalk. U kunt in één oogopslag uw AppleTalk-instellingen en TCP/IP-instellingen naast elkaar zien, waaronder het via DHCP verkregen IP-adres. Bovendien kunt u er IP-adressen en machinenamen op het Internet mee opzoeken en uitzoeken wat de mailserver ('MX') van een bepaald domein is.



Figuur 108: OTTool-infovenster



Figuur 109: OTTool-hoofdvenster

Met de knop 'DNS' kunt u het IP-adres of de machinenaam bij een gegeven machinenaam resp. IP-adres terugvinden.

Met 'Ping' kunt u kijken of de machine bereikbaar is. Let wel op dat beveiligingsfilters ook de oorzaak van *geen reactie* kunnen zijn

Met 'Trace' kunt u nagaan hoe het verkeer naar een bepaalde machine loopt.

Met 'Scan' kunt u zoeken naar andere machines in het netwerk.

Met 'MX' zoekt u voor een op te geven domein naar de mailmachines.

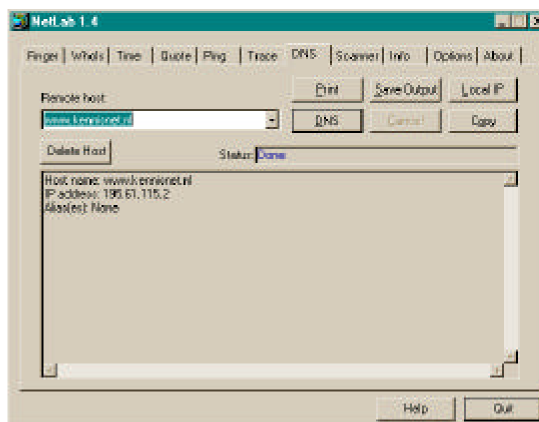
U kunt OTTool ophalen van de site van Neon: http://www.neon.com/.

1.26.2 NetLab

Met NetLab voor Windows 95/98/NT kunt u, net als met OTTool, diverse netwerkdiensten raadplegen. NetLab is eigenlijk wat uitgebreider dan OTTool, op de DNS-functie na. U kunt namelijk geen mailmachine voor een domein opzoeken (helaas).

NetLab biedt verdeeld over de verschillende tabbladen vele functies en uitgebreide informatie.

Met NetLab kunt u trouwens ook de klok van uw computer synchroniseren met andere computers via verschillende protocollen.



Figuur 110: NetLab

U kunt NetLab ophalen op het adres:
ftp://ftp.worldonline.nl/pub/ZDNet/NETLAB.zip.

Hoofdstuk 2. Netwerkadressen

In dit hoofdstuk worden twee veelvoorkomende vragen behandeld met betrekking tot de te gebruiken netwerkadressen.

2.1 Welke adressen worden via DHCP uitgedeeld en welke kan ik zelf indelen?

De reeks adressen die een school krijgt toegewezen, kan in een aantal stukken worden opgedeeld:

- de router;
- één gereserveerd adres;
- werkplekken;
- lokale servers die vanaf kennisnet bereikbaar moeten zijn;
- lokale servers die niet vanaf kennisnet bereikbaar moeten zijn, en overige netwerkapparatuur.

De router heeft altijd het eerste adres uit de reeks. De exacte indeling van het netwerk kunt u nalezen in deel I van het Handboek kennisnet, of snel narekenen op http://enbvlists.kennisnet.nl/techniek/.

2.2 Wat zijn de adressen van…

…de mailserver, newsserver etc.? Indien u van DHCP gebruikmaakt, wordt een deel van de adressen die u nodig hebt voor communicatie met kennisnet, automatisch ingevuld. Om gebruik te kunnen maken van e-mail, discussiegroepen (news), WWW en FTP, zijn echter nog speciale instellingen nodig.

Service	Naam of IP-adres	Poort
Mail versturen	smtp.kennisnet.nl	25
Mail ophalen	pop.kennisnet.nl	110
	imap.kennisnet.nl	143
Discussiegroepen	news.kennisnet.nl	119
Proxy [9]	proxy.kennisnet.nl	8080
Socks [10]	socks-proxy.kennisnet.nl	1080
RTSP-proxy (videoproxy)	rtsp-proxy.kennisnet.nl	554
RTSP-server (videoserver)	video.kennisnet.nl	554
FTP-proxy	ftp-proxy.kennisnet.nl	21
DNS	212.178.5.4	
	212.178.5.5	

Om de tijd van uw PC correct te laten lopen, kunt u ook gebruikmaken van de tijdservers van kennisnet. De proxies beschikken beide over de juiste tijd en kunnen worden gebruikt om de klok van uw computers gelijk te zetten via het Network Time Protocol via het onderliggende Simple Network Time Protocol.

Service	Naam of IP-adres	Poort
Tijdserver	time.kennisnet.nl	(S)NTP

[9] Voor HTTP (WWW), 'beveiligd' (WWW), FTP, Gopher.

[10] Voor IRC, telnet.

Hoofdstuk 3. Foutmeldingen

3.1 E-mail

3.1.1 Fouten tijdens de bezorging van e-mail

Nummer	Engelse melding	Nederlandse omschrijving
421	<*domein*> Service not available, closing transmission channel	Er is een probleem opgetreden of de dienst is tijdelijk niet beschikbaar (mogelijk voor onderhoud), waardoor het e-mailbericht niet kan worden afgeleverd op de betreffende machine.
450	Requested mail action not taken: mailbox unavailable	De postbus waar het bericht moet worden afgeleverd, kan op dit moment niet worden benaderd, mogelijk omdat het betreffende bestand op dit moment in gebruik is door een ander proces op de ontvangende machine.
451	Requested action aborted: local error in processing	Er is een (onbekende) fout opgetreden tijdens het verwerken van het bericht. Bijvoorbeeld omdat het ontvangende systeem niet correct is ingesteld.
452	Requested action not taken: insufficient system storage	Het bericht kon niet worden afgeleverd, omdat de opslagruimte op de ontvangende machine onvoldoende is. Mogelijk is uw bericht erg groot.
500	Syntax error, command unrecognized	Tijdens de communicatie tussen een zendende en een ontvangende machine is er een ongeldig commando aangeroepen, dat de ontvangende machine niet begrijpt. Dit kan duiden op een fout in de software in één van beide computers.
501	Syntax error in parameters or arguments	Een bepaald commando in de onderhandelingen tussen een zendende en een ontvangende machine is aangeroepen met verkeerde parameters.
	<*e-mailadres*>... Sender domain must exist	Dit is één voorbeeld van een '501'-foutmelding. In dit geval wordt het e-mailadres van de ontvanger niet correct doorgegeven. Controleer of u uw e-mailadres, en met name het domein, correct hebt ingevuld in uw e-mailprogramma.
502	Command not implemented	Een aangeroepen commando is op de ontvangende machine niet geïmplementeerd en kan dus niet worden uitgevoerd. Wellicht betreft het een niet-standaard of niet-vereist commando voor correct functioneren. U zou deze fout eigenlijk niet mogen zien en mailservers moeten dit onderling oplossen.
503	Bad sequence of commands	De volgorde waarin tijdens de onderhandeling tussen een verzendende en een ontvangende machine commando's worden uitgevoerd, wordt door de ontvangende machine niet geaccepteerd. Dit duidt mogelijk op fouten in de software van de zendende machine. Normaal zou de gebruiker deze melding niet mogen krijgen.

504	Command parameter not implemented	Een commando is tijdens de onderhandeling tussen een verzendende en een ontvangende machine aangeroepen met opties die niet door de ontvangende machine worden ondersteund.
550	Requested action not taken: mailbox unavailable	Het bericht kan niet worden afgeleverd, omdat de betreffende postbus niet beschikbaar is. Dit kan worden veroorzaakt doordat de postbus niet bestaat of doordat er onvoldoende rechten zijn om de postbus te openen en het bericht te plaatsen.
	<*e-mailadres*>... Relaying denied	Eén voorbeeld van de melding '550' is weigering van het doorzenden van e-mail. U probeert een bericht te bezorgen, waarvan noch de afzender, noch de ontvanger binnen een door de server geaccepteerd domein vallen. Zie ook deel VII, Hoofdstuk 1.
551	User not local; please try <*ander adres*>	De gebruiker aan wie getracht wordt het bericht te zenden, is niet bekend op de betreffende machine. Er wordt mogelijk een alternatief adres gesuggereerd.
552	Requested mail action aborted: exceeded storage allocation	Het bericht kan (tijdelijk) niet worden bezorgd, omdat de postbus van de ontvanger vol is. Zodra de ontvanger zijn postbus opschoont, kan er weer post worden bezorgd. Controleer eventueel hoe groot het verzonden bericht is; indien dit bericht *echt* te groot is voor de ontvangende postbus, zult u het niet kunnen verzenden.
553	Requested action not taken: mailbox name not allowed	Het bericht kon niet worden bezorgd, omdat er een ongeldige naam voor de postbus is opgegeven. Controleer of het e-mailadres correct is ingevoerd.
554	Transaction failed	Het overzenden van het bericht tussen twee machines is niet gelukt. Controleer de inhoud van het foutbericht. Mogelijk hoeft het bericht (nog) *niet* opnieuw te worden verzonden, maar zal een tussengelegen machine nog enkele uren of zelfs dagen proberen om het bericht alsnog af te leveren.

3.1.2 Andere (fout)meldingen in de e-mail

Melding	**Betekenis**
Your mailbox has exceeded its size limit	U hebt teveel e-mail in uw postbus ('mailbox') staan. Probeer om oude berichten of berichten die u niet meer nodig hebt, weg te gooien om zo ruimte vrij te maken. Eventueel kunt u proberen om uw e-mail lokaal, d.w.z. op uw eigen computer of diskettes, op te slaan.
The following addresses had successful delivery notifications <*lijst met e-mailadressen*>	Er is niets aan de hand. U hebt waarschijnlijk om een ontvangstbevestiging gevraagd, welke u in dit bericht krijgt. In het bericht is een lijst gegeven met adressen waar het bericht met succes is afgeleverd.
Non-Delivery Report; Could not deliver message (ID=<*getal*>).	Het bericht dat u hebt verzonden, kon niet worden afgeleverd, bijvoorbeeld omdat de gebruikersnaam niet correct of onbekend is op het ontvangende systeem.

3.2 WWW

Hieronder volgt een lijst van bekende foutmeldingen die webservers kunnen geven, met hun betekenis.

Nummer	Engelse melding	Nederlandse omschrijving
300	Multiple Choices	De opgevraagde informatie is in verschillende representaties (formaten) beschikbaar. Er wordt een lijst gegeven van de verschillende representaties en het bijbehorende adres, zodat de gebruiker een keuze kan maken voor de gewenste representatie.
301	Moved Permanently	De opgevraagde informatie is verplaatst naar een nieuw adres. Verzoeken zouden in het vervolg naar één van de geretourneerde nieuwe adressen moeten gaan. Normaliter zal uw bladerprogramma automatisch doorgaan naar één van de opgegeven adressen.
302	Moved Temporarily	De opgevraagde informatie is tijdelijk verplaatst naar een ander adres. Verzoeken zouden voorlopig naar één van de geretourneerde adressen moeten gaan. Normaliter zal uw bladerprogramma automatisch doorgaan naar één van de opgegeven adressen.
303	See Other	De gezochte informatie is te vinden op een ander adres. Normaliter zal uw bladerprogramma automatisch doorgaan naar het opgegeven adres.
304	Not Modified	Deze melding zou de *menselijke* gebruiker niet moeten zien. Deze melding geeft aan dat, wanneer een stuk informatie *opnieuw* wordt opgevraagd om te controleren of deze inmiddels is gewijzigd, de informatie nog ongewijzigd is.
305	Use Proxy	De opgevraagde informatie kan alleen via de opgegeven proxyserver worden benaderd. Normaliter zal uw bladerprogramma deze melding afhandelen.
400	Bad Request	Het verzoek om informatie kon niet worden ingewilligd, omdat er een fout zit in de adressering van de informatie (een ongeldig adres). Corrigeer het adres en probeer het opnieuw.
401	Unauthorized	U bent niet bevoegd om de gevraagde informatie te raadplegen. U hebt hier waarschijnlijk een gebruikersnaam en wachtwoord voor nodig.
402	Payment Required	Deze melding geeft aan dat er op de een of andere wijze een elektronische betaling moet plaatsvinden voordat u de gevraagde informatie kunt raadplegen.
403	Forbidden	U mag, om al dan niet nader verklaarde redenen, de betreffende informatie niet raadplegen. Een mogelijkheid is dat u de informatie probeert te raadplegen vanaf een onbevoegde machine.
404	Not Found	U hebt geprobeerd een bepaalde webpagina of een andere informatie op te vragen, maar de webserver kon de informatie niet vinden. Mogelijk hebt u een oude verwijzing gevolgd of een verkeerd adres ingetypt.

405	Method Not Allowed	Deze melding geeft aan dat uw bladerprogramma op de verkeerde wijze een verzoek heeft ingediend om de gewenste informatie op te vragen. Mogelijk komt dit doordat er in de verwijzende pagina een fout zit.
406	Not Acceptable	De webserver is niet in staat om de opgevraagde informatie in een formaat te leveren, dat uw bladerprogramma kan verwerken.
407	Proxy Authentication Required	U dient zich eerst aan te melden bij de proxyserver voordat u de informatie kunt opvragen. Waarschijnlijk krijgt u een venster gepresenteerd, waarin u een naam en wachtwoord dient in te vullen. Deze melding zal verschijnen indien het niet lukt om aan te melden.
408	Request Timed Out	Het verzoek kon niet worden behandeld binnen de tijd die de server handhaaft als maximale wachttijd. Mogelijk is de server te zwaar belast of is een berekening die de server moet uitvoeren om de gewenste informatie te presenteren, erg complex en tijdrovend. U kunt eventueel op een later tijdstip proberen om de informatie alsnog op te vragen.
409	Conflict	Er is een probleem opgetreden bij het benaderen van de informatie op de server. Mogelijk is iemand anders net bezig om de informatie te wijzigen, waardoor de server de informatie niet kan raadplegen. Waar mogelijk zal het bericht voldoende informatie bevatten om het probleem te kunnen achterhalen, hoewel deze informatie mogelijk alleen door terzake kundige personen te begrijpen is.
410	Gone	De opgevraagde informatie is niet langer beschikbaar en er is ook geen alternatief adres bekend.
411	Length Required	Uw bladerprogramma heeft de server niet voorzien van de vereiste informatie over de lengte van het ingediende verzoek. U zou kunnen proberen de informatie met een ander bladerprogramma of een nieuwere versie van uw huidige programma op te vragen.
412	Precondition Failed	Bij het indienen van het verzoek is extra informatie (een aantal voorwaarden) aan het verzoek toegevoegd om de server in staat te stellen om de juiste informatie te vinden. Desondanks bleek de server niet in staat om informatie te vinden, die aan alle gestelde voorwaarden voldoet.
413	Request Entity Too Large	De server weigert om de opgevraagde informatie beschikbaar te stellen, omdat deze te groot in omvang is.
414	Request-URI Too Long	Het ingediende verzoek is van een te grote lengte. Mogelijk is een fout in het opgegeven adres, met teveel extra informatie, geslopen.
415	Unsupported Media Type	De server was niet in staat om de opgevraagde informatie te verwerken en aan u te geven.

500	Internal Server Error	Er is een probleem in de server ontstaan. Waarschijnlijk is er een probleem met een deel van de instellingen of functioneert een script dat dynamisch informatie moet genereren, niet correct. Veelal wordt u bij het optreden van een dergelijke fout gevraagd om de beheerder van de webserver in te lichten.
501	Not Implemented	De server ondersteunt niet de functionaliteit die noodzakelijk is om uw verzoek in te willigen.
502	Bad Gateway	U kunt deze melding krijgen van een server die als 'proxy' of als 'gateway' optreedt, welke een foutmelding of een ongeldige reactie heeft ontvangen van de machine die de informatie werkelijk bevat.
503	Service Unavailable	De server is tijdelijk niet beschikbaar, wegens overbelasting of vanwege onderhoud. U kunt op een later tijdstip proberen de informatie alsnog op te vragen.
504	Gateway Timeout	U kunt deze melding krijgen van een server die als 'proxy' of als 'gateway' optreedt, welke niet op tijd de gevraagde informatie heeft ontvangen van de machine die de informatie werkelijk bevat.
505	HTTP Version Not Supported	Uw bladerprogramma heeft getracht met de server te communiceren in een versie van het HTTP-protocol, die (nog) niet door de server wordt ondersteund.

3.3 FTP

Nummer	Engelse melding	Nederlandse omschrijving
202	Command not implemented, superfluous at this site.	Het commando dat uw FTP-programma aan de FTP-server heeft doorgegeven, is niet geïmplementeerd op de FTP-server omdat het een overbodig commando zou zijn.
331	User name okay, need password.	De opgegeven gebruikersnaam is geaccepteerd, maar er is nog een wachtwoord vereist.
332	Need account for login.	De opgegeven gebruikersnaam en het wachtwoord zijn geaccepteerd, maar u dient nog een 'accountnaam' op te geven om u te kunnen aanmelden.
421	Service not available, closing control connection.	De dienst is niet beschikbaar en de verbinding is verbroken. Dit antwoord kan op vrijwel elke opdracht worden gegeven wanneer het systeem weet dat het moet afsluiten.
425	Can't open data connection.	Het is niet gelukt om een dataverbinding te openen. Om dit te begrijpen, is enig begrip van het FTP-protocol vereist. FTP gebruikt twee 'kanalen': één kanaal wordt voor de besturing gebruikt, het andere voor de overdracht van gegevens. Het tweede kanaal wordt echter pas geopend op het moment dat dit vereist is, en is niet gebonden aan een vast poortnummer. Indien op de zendende of de ontvangende machine geen poort meer beschikbaar is, kan deze melding worden gegeven.

426	Connection closed; transfer aborted.	De verbinding is verbroken, omdat de overdracht is afgebroken
450	Requested file action not taken. File unavailable (e.g., file busy).	Het opgevraagde bestand is niet beschikbaar. Mogelijk bestaat het bestand wel, maar is het in gebruik door een ander proces op de FTP-server.
451	Requested action aborted: local error in processing.	De uitvoering van een verzoek is afgebroken, omdat er een fout is opgetreden in de verwerking van de gegevens.
452	Requested action not taken. Insufficient storage space in system.	Een verzoek is niet uitgevoerd, omdat er onvoldoende schijfruimte is op de FTP-server.
500	Syntax error, command unrecognized.	Er is een fout geconstateerd in het opgegeven commando. Dit kan duiden op een fout in uw FTP-programma, maar het kan ook betekenen dat er een te lang commando is gegeven, waar de FTP-server niet mee overweg kan.
501	Syntax error in parameters or arguments.	De parameters of aanvullende informatie bij een opgegeven commando zijn niet correct geformuleerd.
502	Command not implemented.	Uw FTP-programma heeft een commando aan de FTP-server gegeven, dat niet is geïmplementeerd op de FTP-server; waarschijnlijk betreft het een commando dat volgens de specificaties niet verplicht hoeft te worden geïmplementeerd.
503	Bad sequence of commands.	De volgorde waarin uw FTP-programma een aantal commando's heeft aangeroepen, is niet correct.
504	Command not implemented for that parameter.	Het commando dat uw FTP-programma heeft gegeven aan de webserver, kan normaliter wel worden uitgevoerd, maar is niet beschikbaar met de opgegeven parameters.
530	Not logged in.	U probeert een opdracht uit te voeren, waarvoor u zich eerst dient aan te melden. Mogelijk is het u niet opgevallen dat de aanmelding niet is geslaagd. Probeer alsnog aan te melden en opnieuw uw opdracht uit te laten voeren.
532	Need account for storing files.	Voor sommige systemen dient u, zoals in het geval dat u deze melding krijgt, een 'accountnaam' op te geven bij het aanmelden. Probeer opnieuw aan te melden op het systeem, met vermelding van de vereiste accountnaam, en probeer dan opnieuw uw bestand op de FTP-server op te slaan.
550	Requested action not taken. File unavailable.	De gevraagde actie kon niet worden uitgevoerd, omdat het bestand waarop de actie betrekking heeft, niet beschikbaar is. Mogelijk bestaat het bestand niet of niet meer, of u hebt onvoldoende rechten om de actie op het bestand uit te voeren.
551	Requested action aborted: page type unknown.	De gevraagde actie is afgebroken. De overdracht van gegevens wordt in 'pagina's' verdeeld, waarbij voor een pagina een voor de server onbekend type is opgegeven. Waarschijnlijk zijn uw FTP-programma en de FTP-server niet compatibel.

552	Requested file action aborted. Exceeded storage allocation (for current directory or dataset).	De gevraagde actie die u wilde uitvoeren op een bepaald bestand, is afgebroken. De beschikbare opslagruimte is onvoldoende voor de huidige map of gegevensverzameling.
553	Requested action not taken. File name not allowed.	U hebt geprobeerd een bestand te verzenden naar de FTP-server of om de naam van een bestand op de FTP-server te wijzigen, maar er komen waarschijnlijk karakters in voor, die de FTP-server niet aan kan.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonische te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u een e-mail sturen aan 'handboek@kennisnet.nl'.

Index

R

S

T

U

W

Z

Figurenlijst

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel IV, Diensten

Indeling van dit document

Dit document behandelt een aantal speciale diensten.

Hoofdstuk 1 behandelt het gebruikers- en groepenbeheer. De centrale database van kennisnet kunt u onderhouden via een webinterface.

In Hoofdstuk 2 wordt uitgelegd hoe u uw plek in het webhotel kunt onderhouden. Tevens worden enkele tips gegeven over websites met handige tips en hulpmiddelen.

Inhoudsopgave

Hoofdstuk 1. Gebruikers- en groepenbeheer

In dit hoofdstuk wordt uitgelegd hoe u, als ICT-coördinator, gebruikers van kennisnet binnen uw organisatie kunt beheren. Voor het beheer van gebruikers hebt u een e-mailprogramma en een bladerprogramma nodig. In deel III wordt uitgelegd hoe u deze kunt gebruiken.

DE EERSTE KEER…

Voor het allereerste gebruik krijgt u de persoonlijke gegevens voor de ICT-coördinator:

- gebruikersnaam (bijv. jan.voorbeeld.school.plaats)
- wachtwoord (bijv. 2FK4YA84)
- postbusnummer (bijv. jan.voorbeeld@school.plaats.kennisnet.nl)

Deze ontvangt u per brief. Met deze gegevens kunt u naar http://www.beheer.kennisnet.nl/. Hier vind u informatie over hoe u de namen van de leerlingen en docenten kunt aanleveren ten behoeve van e-mail op naam. Als uw instelling geen prijs stelt op e-mail en gebruikersnamen waar de naam van de gebruikers in voorkomt, dan kunt u hier ook anonieme adressen op nummer aan laten maken.

Om e-mail op naam in te voeren, hebben we van de instelling een aantal gegevens nodig over de eindgebruikers. Deze gegevens moeten door u aangeleverd worden. Deze gegevens kunt u bijvoorbeeld halen uit de schooldatabase, of een systeem waarin uw instelling de gegevens heeft vastgelegd. Als u deze gegevens kopieert naar bijvoorbeeld Excel, kunt u daar het bestand opslaan als ‘comma separated values’ (door komma's gescheiden waarden). U ontvangt van ons een bestand retour dat voorzien is van gebruikersnamen en wachtwoorden en e-mailadressen. U kunt dit gebruiken om aan de gebruikers te melden wat hun gebruikersnaam en wachtwoord is. **Bewaar dit document goed, maar wel zó, dat onbevoegden er niet bij kunnen!**

U kunt de gegevens van de gebruikers beheren via een 'webinterface' met uw bladerprogramma. Vraag daartoe de startpagina op: http://www.beheer.kennisnet.nl/. Dit werkt overigens alleen *binnen* kennisnet en is niet toegankelijk via het Internet!

Wijzig uw wachtwoord

E-mailprogramma’s vragen bij het configureren om het kennisnetwachtwoord. Het is dan handig om, indien u een ander wachtwoord wilt gebruiken dan hetgeen u is toegestuurd, eerst uw wachtwoord te veranderen in het door u gewenste wachtwoord voordat u de e-mail gaat configureren. Voor het veranderen van een wachtwoord vraagt u de volgende webpagina op in uw bladerprogramma: http://www.beheer.kennisnet.nl/wachtwoord/.

Configureren e-mail

E-mailprogramma’s beschikken over invoervelden voor een gebruikersnaam, e-mailprotocol, mailserver en een wachtwoord. Om toegang tot deze invoervelden te verkrijgen, moet voor elk e-mailprogramma anders gehandeld worden. Lees de handleiding van uw e-mailprogramma voor de juiste handelingen die uitgevoerd moeten worden om toegang te krijgen tot de bovengenoemde invoervelden. Voor enkele programma's wordt reeds uitleg gegeven in deel III van Het Handboek.

TOEDELEN POSTBUSNUMMERS BINNEN DE SCHOOL

Wat staat er in de e-mail?

De e-mail met postbusnummers die klaarstaat in uw postbus, bevat een lijst met de volgende gegevens (*voorbeeld*):

```
gebruikersnaam,               wachtwoord,   e-mailadres
jan.voorbeeld.school.plaats,  giraffe,      jan.voorbeeld@school.plaats.kennisnet.nl
```

BEHEER VAN POSTBUSSEN

Hoe beheert u de postbuslijst van uw school?

Voor het beheer van de postbuslijst is het wenselijk om de e-mailadressen vanuit de e-mail over te brengen naar een spreadsheetprogramma, bijvoorbeeld Excel. Voer hiervoor de volgende handelingen uit.

- Bewaar het e-mailbericht met gegevens als een tekstbestand naar een plaats die bereikbaar is vanuit uw spreadsheetprogramma.
- Start uw spreadsheetprogramma en open met ‘File’/'Bestand' en ‘Open’ uit de menubalk het tekstbestand met de gegevens.
- Geef aan vanaf welke regel u het tekstbestand op wilt nemen in uw spreadsheet.
- Geeft aan dat de velden door komma’s gescheiden worden.
- Voltooi het openen van het tekstbestand.
- De gebruikersgegevens zijn nu opgenomen in uw spreadsheet.

U kunt deze spreadsheet bijvoorbeeld gebruiken om de gegevens te verspreiden onder de gebruikers. Het is van belang dat deze lijst met namen en postbusnummers bijgewerkt is en dat er een reservekopie van aanwezig is.

Wachtwoorden

Wachtwoorden zijn persoonlijk en geven toegang tot persoonlijke gegevens. Het is daarom niet wenselijk dat een gebruikersnaam met wachtwoord gebruikt kan worden door een andere gebruiker dan aan wie het toebedeeld is. Als wachtwoorden makkelijk te raden of te achterhalen zijn, bestaat het gevaar dat personen zich op kennisnet kunnen voordoen als iemand anders. Hierdoor wordt het onmogelijk om onrechtmatig gebruik van kennisnet te traceren. Scholen moeten rekening houden met deze problematiek bij het opstellen van richtlijnen voor wachtwoordgebruik binnen de school.

Moeilijk te kraken wachtwoorden bevatten geen bestaande woorden en zijn een combinatie van cijfers en letters met een lengte van ten minste acht karakters. Om dergelijke wachtwoorden makkelijk te onthouden, kan gebruikgemaakt worden van een bekende zin. Bijvoorbeeld: “Heb je wel gehoord van de zevensprong” wordt Hjwgvd7s.

Wachtwoord vergeten?

Als een gebruiker het wachtwoord vergeten is, dan kunt u – als ICT-coördinator – aan deze gebruiker een nieuw wachtwoord toekennen. Voor het invoeren van een nieuw wachtwoord maakt u gebruik van de volgende webpagina: http://www.beheer.kennisnet.nl/, onder het kopje ‘Wijzigen gebruikersgegevens’.

Hoofdstuk 2. Onderhoud van het webhotel

In dit hoofdstuk wordt uitgelegd hoe u uw webpagina's in het webhotel van kennisnet kunt onderhouden. Hoewel deze informatie wellicht gedeeltelijk toepasbaar is op andere, externe websites, is de hier gepresenteerde informatie specifiek voor de situatie van kennisnet bedoeld.

Wanneer u 'webhosting' aanvraagt, hebt u de keuze uit twee vormen:

- Standaard web: gebaseerd op een Sun Solaris-systeem met de Netscape webserver en enkele standaardscripts en CGI-applicaties om te gebruiken vanuit uw webpagina's;
- FrontPage® Web: gebaseerd op een Windows NT-systeem, waarop FrontPage-extensies worden ondersteund.

In dit hoofdstuk wordt gebruikgemaakt van een fictieve school, namelijk de Voorbeeldschool in Zoetermeer, met als BRIN-nummer '99ZZ'.

Let op dat u *uw eigen* BRIN-nummer invult bij de genoemde gebruikersnamen, voorzover dit voor u van toepassing is!

Streaming Media

Een beschrijving over de toegang tot de Streaming Media-server en het gebruik van Streaming Media-bestanden vindt u binnenkort in de meest recente versie van Het handboek op kennisnet `http://www.kennisnet.nl/`, onder 'Servicepunt'.

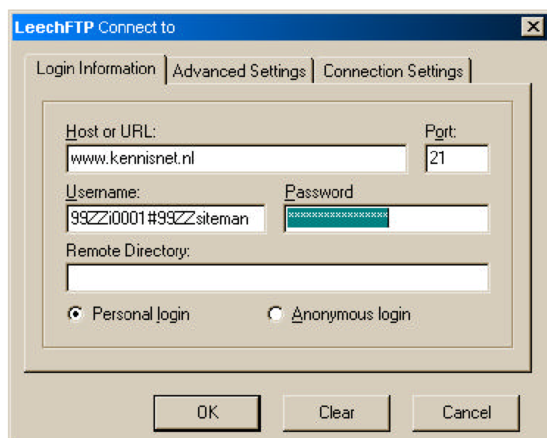
STANDAARD WEB

Voor het standaard web kunt u de webpagina's onderhouden via FTP. U kunt de pagina's op uw eigen computer ontwikkelen en vervolgens versturen naar de webserver met een FTP-programma naar keuze. Voor de instellingen van uw FTP-programma wordt verwezen naar deel III.

Toegangscontrole

Voor de toegangscontrole op de website wordt gebruikgemaakt van dezelfde mechanismen als voor e-mail en dergelijke. In de centrale LDAP-server is voor iedere school of instelling een groep aangemaakt, waarin de personen zijn vertegenwoordigd die de website mogen onderhouden. De naam van deze groep bestaat uit het BRIN-nummer van de school en de term 'siteman', dus – in dit voorbeeld – '99ZZsiteman'.

Standaard zijn de eerste vier ICT-coördinatoren van de school in deze groep vertegenwoordigd. Het is mogelijk om deze groep aan te passen, zoals wordt uitgelegd in Hoofdstuk 1. In dit voorbeeld mogen de personen met de gebruikersidentiteit '99ZZi0001' tot en met ‘'99ZZi0004' de website onderhouden. Het is ook mogelijk dat er gebruikersnamen worden gebruikt met (een deel van) uw echte naam en de (domein)naam van de school erin, bijvoorbeeld 'jan.de.vries.voorbeeldschool.nl'. Dit hangt af van uw instellingen (zie wederom Hoofdstuk 1).



Om u aan te melden, dient u in uw FTP-programma als gebruikersnaam op te geven uw eigen gebruikersnaam (bijvoorbeeld '99ZZi0001'), gevolgd door een 'hekje' (#) en de groepsnaam (bijvoorbeeld '99ZZsiteman').

Het wachtwoord is het wachtwoord dat bij de gebruikersnaam hoort, zoals dat ook voor uw e-mail van toepassing is.

Na het aanmelden komt u, indien u zelf geen andere map hebt opgegeven, in de hoofdmap van de website van uw school terecht, waar u de bestanden kunt plaatsen.

Figuur 1: aanmelden voor onderhoud webhotel

De standaardpagina van uw website en elke submap dient de naam '`index.html`' te hebben. Let op de laatste '`l`'; de bestandsextensie '`.htm`' is in dit geval onvoldoende. Voor alle overige pagina's kunnen zowel beide bestandsextensies '`.htm`' en '`.html`' worden gebruikt.

Uw webpagina bekijken

U kunt met uw bladerprogramma uw webpagina zowel vanaf kennisnet als vanaf Internet bekijken op het adres http://<*schoolnaam*>.<*plaatsnaam*>.kennisnet.nl/. In dit voorbeeld zou het dus http://voorbeeldschool.zoetermeer.kennisnet.nl/ worden. **Dit voorbeeldadres is uiteraard slechts een fictief adres en bestaat niet echt!**

Indien u tevens een eigen domeinnaam hebt aangevraagd, zal uw website, indien deze naam is toegekend en doorgevoerd in de systemen van kennisnet, ook op die manier toegankelijk zijn.

Scripts

Voor gebruikers van het standaard web is een aantal scripts beschikbaar gesteld om te gebruiken op uw website. De scripts zijn te gebruiken voor:

- formulieren, om invulformulieren te versturen;
- paginateller, om te tellen hoeveel personen uw pagina hebben bezocht;
- prikbord, waar gebruikers berichtjes kunnen plaatsen.

Uitleg over het gebruik van de scripts en voorbeelden vindt u op het adres http://www.kennisnet.nl/educatiefnet/scripts.html.

FrontPage® web

Dit is een beknopte handleiding van de werking van de FrontPage Client en hoe u hiermee uw website kunt onderhouden. In deze paragraaf worden de volgende onderwerpen behandeld.

- Wat is FrontPage?
- Beginnen met FrontPage.
- Maken van een website.
- De eerste pagina.
- Beheren van de website.

In de daaropvolgende paragrafen wordt dieper ingegaan op de volgende onderwerpen.

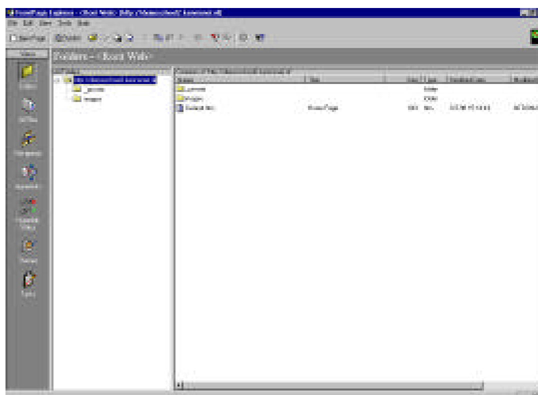
- FrontPage Explorer
- FrontPage Editor

Wat is FrontPage?

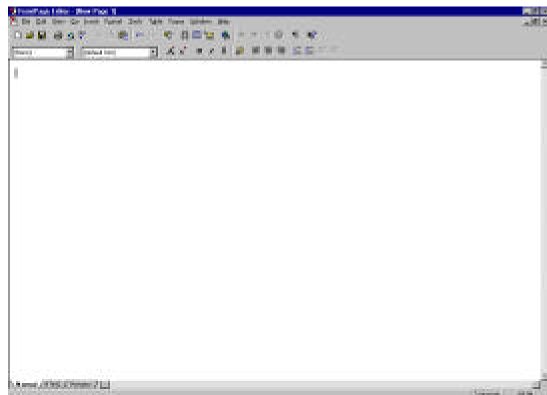
FrontPage is een programma om op een eenvoudige manier websites te maken en te beheren. FrontPage biedt hiervoor verschillende onderdelen.

- FrontPage Explorer
- FrontPage Editor
- Microsoft Image Composer

U kunt uw website eenvoudig bekijken, beheren en besturen met behulp van de grafische tools van de ingebouwde FrontPage Explorer. FrontPage Explorer biedt u bijvoorbeeld een duidelijk inzicht in de structuur van uw website en van de daarin opgenomen hyperlinks (Figuur 2). Meer functies van FrontPage Explorer vindt u op bladzijde 11 (FrontPage Explorer).



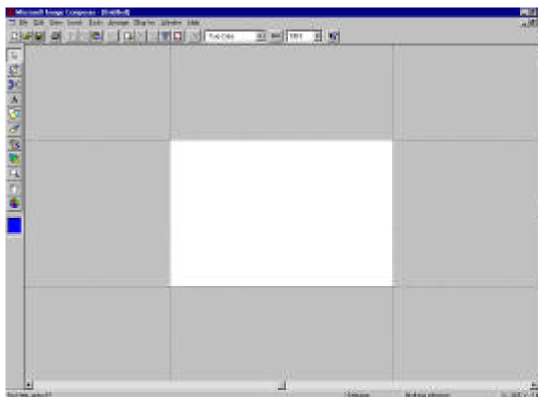
Figuur 2: Frontpage-hoofdscherm



Figuur 3: FrontPage Editor

Het aanbrengen van hyperlinks en het toevoegen van informatie uit applicaties of gegevensbestanden gaat als vanzelf met de zeer visuele FrontPage Editor (Figuur 3).Voor een uitgebreide beschrijving kunt u terecht op pagina 10 ('De eerste pagina').

Met Microsoft Image Composer kunt u zelf illustraties maken voor uw website of er foto's in opnemen (Figuur 4). Dit programma staat op de FrontPage CD-ROM en kan samen met de FrontPage Client worden geïnstalleerd.



Figuur 4: Image Composer

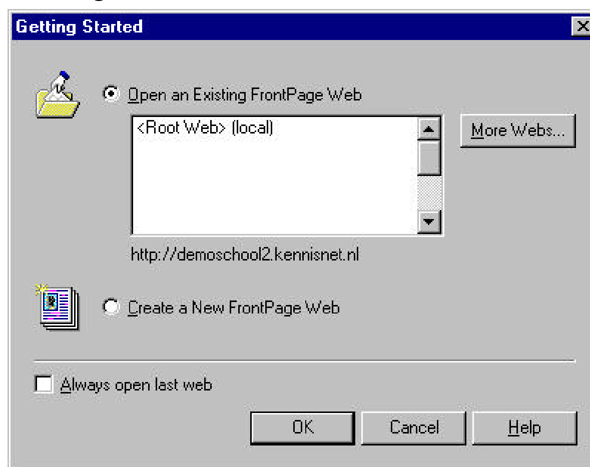
Beginnen met Frontpage

Er wordt hier vanuit gegaan dat de FrontPage Client reeds is geïnstalleerd. Er is alleen een Engelse versie beschikbaar. Om een nieuwe website op te bouwen, gaat u als volgt te werk.

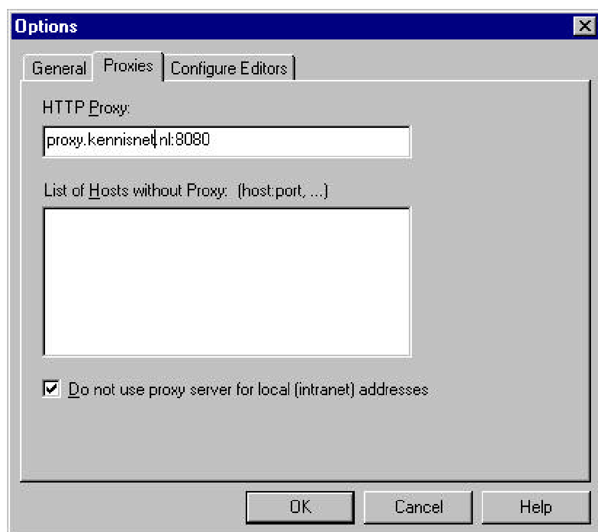
Start de FrontPage Client via het 'Start'-menu van Windows. Het volgende scherm, zoals weergegeven in Figuur 5, verschijnt.

U kunt hier aangeven of u met een bestaande website of een nieuwe website aan de slag wilt.

Indien u dit nog niet heeft ingesteld en vanuit kennisnet uw website bijwerkt, dient u echter eerst de instellingen voor de webproxy in te vullen. Klik dan eerst op 'Cancel'. Het scherm van de FrontPage Explorer verschijnt. Selecteer uit het menu 'Tools' de keuze 'Options…'. Er verschijnt een venster, zoals in Figuur 6.



Figuur 5: startvenster ('Getting Started')



Figuur 6: proxy-instellingen

Ga naar het tabblad 'Proxies'. In het veld 'HTTP Proxy:' dient u het adres van de proxies van kennisnet in te vullen, gevolgd door een dubbele punt en het poortnummer: `proxy.kennisnet.nl:8080`.

Klik op 'OK' om de instellingen te activeren.

U bevindt zich weer in de FrontPage Explorer. Selecteer uit het menu 'File' de keuze 'Open FrontPage Web'. Er verschijnt weer een venster zoals in Figuur 5.

Klik op de knop 'More Webs…'. Vervolgens verschijnt wederom het venster zoals getoond in Figuur 7.

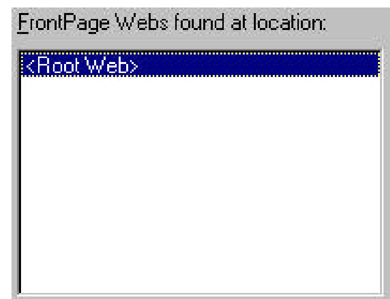


Figuur 7: Open FrontPage Web

Vul bij: ‘Select a Web server or disk location’ de naam in van de website (het Internetadres) zoals u die van kennisnet heeft gekregen. Dit is, volgens de geldende standaard, een naam in de vorm van: ‘<*schoolnaam*>.<*plaatsnaam*>.kennisnet.nl’.

Druk vervolgens op de knop: 'List webs'. In het venster: 'FrontPage Webs found at location:' verschijnt een lijst van de websites.

Dubbelklik op <Root Web>.



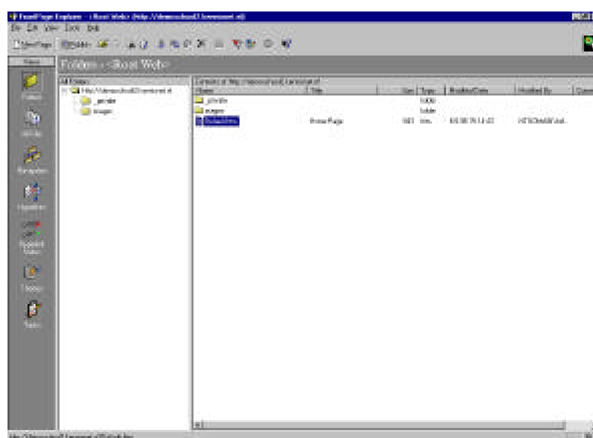
Figuur 8: lijst met locaties

In het scherm dat nu verschijnt, kunt u een loginnaam en wachtwoord invoeren (Figuur 9). Vul hier de gebruikersnaam en het wachtwoord in die u hebt gekregen van kennisnet.

Het FrontPage Explorer-scherm verschijnt, waarmee u kunt navigeren binnen uw website.



Figuur 9: aanmelden voor FrontPage



Figuur 10: FrontPage Explorer

De eerste pagina

Zodra u uw website hebt geopend, is het mogelijk om pagina's aan te maken of te bewerken. Het scherm van de FrontPage Explorer lijkt op dat van de verkenner van Windows 95/98 of Windows NT-verkenner.

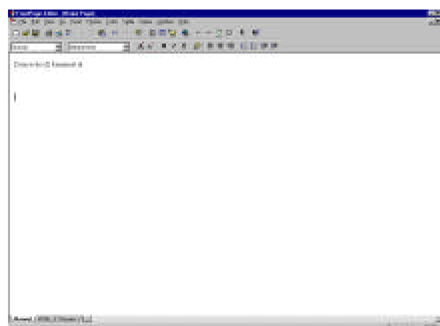
Rechts bevindt zich het scherm waarin u de bestanden kunt zien ('Contents' of '`http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/`'). Aan de linkerkant ziet u een boomstructuur zoals u die ook kent van de verkenner (All folders). Hier kunt u bladeren door de mappen die zich op uw webserver bevinden. In het venster aan de rechterkant kunt u vervolgens op de pagina's dubbelklikken om die te bewerken.

Ook is het mogelijk om een nieuwe pagina aan te maken. Hiervoor klikt u met de rechtermuisknop in het rechter scherm. Selecteer vervolgens: ‘New page’. Er wordt een nieuwe pagina aangemaakt die u vervolgens een naam kunt geven. Als u vervolgens op de naam dubbelklikt, wordt de FrontPage Editor geopend waarmee de pagina kan worden bewerkt.

Standaard staat er een pagina op de webserver die ‘`default.htm`’ heet. Dit is de pagina die de server zal tonen zodra men het adres van uw website in een bladerprogramma intypt: `http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/`.

Deze pagina kunt u naar eigen inzicht aanpassen door erop te dubbelklikken. De FrontPage Editor wordt geopend en de pagina kan worden bewerkt.

Als het de eerste keer is dat de pagina wordt bewerkt, wordt er door kennisnet een pagina aangemaakt waarop de naam van de website staat vermeldt (Figuur 11).



Figuur 11: standaardpagina

De FrontPage Editor is te vergelijken met het tekstverwerkingsprogramma Microsoft Word. Teksten, tabellen en plaatjes kunnen eenvoudig worden ingevoegd zonder dat er kennis van HTML is vereist. Langs de bovenkant van het scherm bevinden zich enkele werkbalken waar de meest gebruikte functies staan. Voor een uitgebreide beschrijving van de Editor kunt u terecht in de helpfunctie van de FrontPage Editor.

Zodra u de pagina naar uw wensen hebt aangepast, kunt u de pagina opslaan door in de werkbalk op de ‘Save’-icoon te drukken. Vanaf dat moment staat de zojuist aangepaste pagina op het Internet.

FrontPage Explorer

Deze subparagraaf is een korte introductie van de FrontPage Explorer. Deze Explorer kan worden vergeleken met de verkenner die wordt geleverd met Windows 95/98 of NT. Het is een grafische representatie van de structuur van de website. Er kan worden gebladerd door de websites, pagina's en mappen kunnen worden aangemaakt. Websites, pagina's en mappen kunnen ook worden gewijzigd of worden verwijderd.

Voor een uitgebreide handleiding kunt u de (Engelstalige) helpfunctie van FrontPage raadplegen.

Er is een aantal manieren om de FrontPage Explorer te gebruiken. Binnen het programma worden dat ‘views’ genoemd. Er zijn verschillende ‘views’ mogelijk.

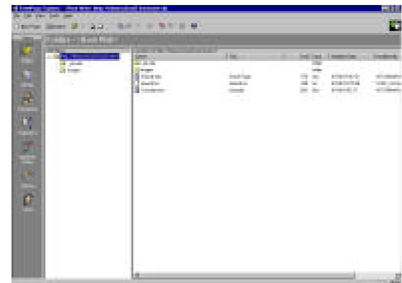
- Folders
- All files
- Navigation
- Hyperlinks
- Hyperlink status
- Themes
- Tasks

Hierna worden de verschillende views besproken.

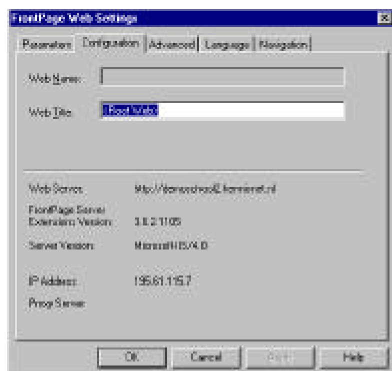
Views

Folders

Dit is de view die automatisch verschijnt zodra u zich succesvol hebt aangemeld op de webserver (Figuur 12). De meeste handelingen zullen vanuit deze view worden gedaan. De view is te vergelijken met de verkenner die standaard zit bij Windows 95/98 of NT. Met aan de linkerkant de boomstructuur van de website en rechts een venster met de inhoud van de website. Pagina's en mappen kunnen aangemaakt, gewijzigd of verwijderd worden. Dit kan door met de rechter muisknop te klikken in het rechter venster. Er verschijnt een menu waar gekozen kan worden uit: 'New Page' (nieuwe pagina) of 'New Folder' (nieuwe map).



Figuur 12: View 'Folders'

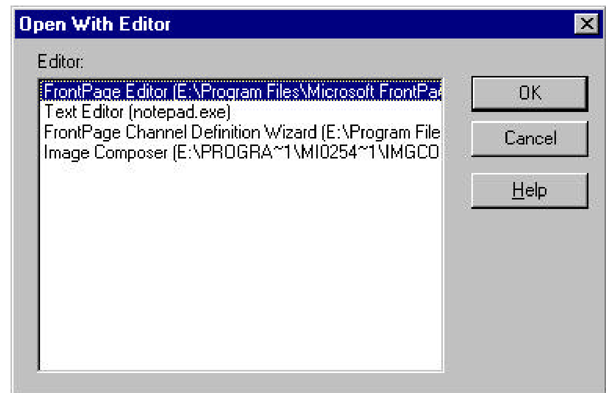


Figuur 13: Web Settings

Verder is er nog een optie die 'Web Settings' heet (Figuur 13). Hier kunnen enkele algemene instellingen voor de website worden veranderd, waaronder de titel van de website.

Als u een document selecteert en vervolgens de rechter muisknop indrukt, krijgt u een ander menu te zien. Hier kan worden gekozen uit de volgende opties.

- **Open**: het document wordt geopend binnen de FrontPage Editor.
- **Open With Editor**: er verschijnt een scherm waar gekozen kan worden met welk programma het document moet worden geopend (Figuur 14). Selecteer het programma waarmee de pagina moet worden geopend en klik op 'OK'.
- **Cut**: de standaardfunctie knippen.
- **Copy**: de standaardfunctie kopiëren.
- **Rename**: het document een nieuwe naam geven.
- **Delete**: het geselecteerde document verwijderen van de website.
- **Add Task**: hier kan worden aangegeven wat er nog aan de geselecteerde pagina gedaan moet worden.
- **Properties**: u kunt hiermee de eigenschappen van de geselecteerde pagina aanpassen. U kunt hier ook een beschrijving geven van de functie van de pagina of een korte samenvatting van de inhoud. Dit kan dan worden teruggevonden binnen de FrontPage Explorer.

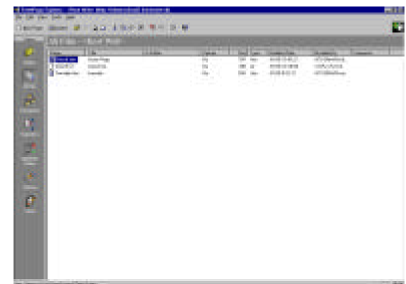


Figuur 14: openen met een extern programma

All files

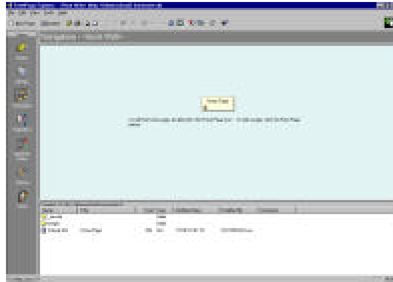
Deze view laat alle bestanden zien die op de website staan, ongeacht de map waar de bestanden staan (Figuur 15).

Door in dit scherm met de rechter muisknop te klikken, kan een nieuwe pagina worden aangemaakt. Ook kan hier de naam van een pagina worden veranderd of kan een pagina of plaatje worden verwijderd, zoals hierboven beschreven. In deze view kunnen geen mappen worden aangemaakt of verwijderd.



Figuur 15: View 'All files'

Navigation



Figuur 16: View 'Navigation'

In deze view is het mogelijk om de navigatie van de website aan te geven (Figuur 16). FrontPage kan automatisch knoppen of hyperlinks genereren naar andere pagina's. Door in dit scherm bestanden te slepen naar het hoofddocument, worden automatisch knoppen en links toegevoegd aan de pagina, die ervoor zorgen dat bezoekers van de website de weg kunnen vinden binnen de website.

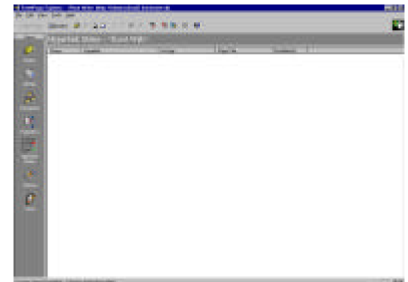
De view bestaat uit twee schermen: het bovenste scherm is een grafische presentatie van de navigatiestructuur. Vanuit het onderste scherm kunnen pagina's die naar elkaar moeten verwijzen, naar de pagina in het bovenste scherm worden ‘gesleept’. Dit kan men doen door in het onderste scherm een pagina te selecteren en vervolgens naar het bovenste scherm te slepen waarbij de linker muisknop ingedrukt wordt gehouden.

Op het moment dat het gesleepte document in de buurt komt van een ander document, verschijnt er een lijn van het ene naar het andere document. Op het moment dat de lijn naar de juiste pagina verwijst, moet de linker muisknop worden losgelaten. In de pagina waar de bewust pagina naartoe is gesleept, komt automatisch een knop die verwijst naar de gesleepte pagina. Zo wordt er door FrontPage automatisch een navigatieboom aangemaakt met hyperlinks of knoppen.

In het onderste scherm kunt u door de website bladeren, zoals ook via de ‘Folders’ view.

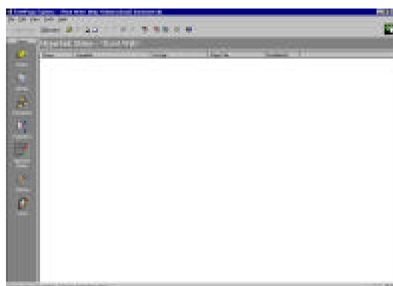
Hyperlinks

In dit scherm kan worden bekeken welke bestanden een link hebben naar de andere pagina's. Op deze manier kan worden bekeken welke invloed bijvoorbeeld het verwijderen van een pagina kan hebben op de andere pagina's.



Figuur 17: View 'Hyperlinks'

Hyperlink status



Figuur 18: View 'Hyperlink status'

In de view ‘Hyperlink status’ wordt bekeken of alle hyperlinks die op de diverse pagina’s staan, nog correct zijn. Hierbij wordt gekeken naar zowel links binnen de website als naar links die naar websites gaan die buiten `http://<schoolnaam>.<plaatsnaam>.kennisnet.nl/` liggen.

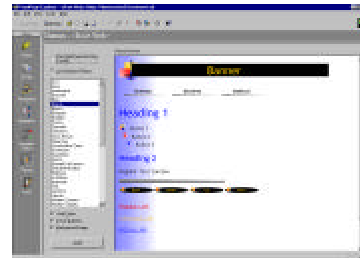
Themes

Frontpage biedt de mogelijkheid om de hele website in een bepaalde opmaak te krijgen. FrontPage heeft hiervoor ‘Themes’ beschikbaar. Deze thema’s kunnen het beste worden vergeleken met de sjablonen zoals die binnen Microsoft Word worden gebruikt. De thema’s bevatten informatie over de opmaak van de gehele website, bijvoorbeeld:

- achtergronden;
- lettertype;
- knoppen;
- animaties;
- kleuren van de tekst.

Op het moment dat een bepaald thema is geselecteerd, heeft de website in één keer een totaal andere opmaak. Door een ander thema te selecteren, kan de website er heel anders uitzien. Standaard worden er door Microsoft enkele thema's meegeleverd. Hieruit kan een keus worden gemaakt.

Links kan men uit een lijst een thema selecteren. Rechts ziet men vervolgens een voorbeeld hoe de website eruit kan komen te zien (Figuur 19). Op het moment dat er op 'Apply' wordt gedrukt, wordt de website volgens het zojuist gekozen thema opgemaakt.

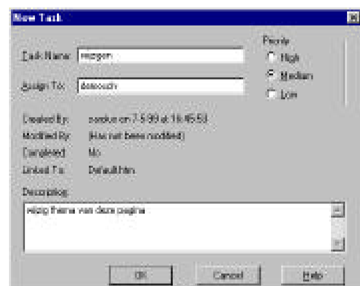


Figuur 19: View 'Themes'

Tasks

In de view 'Tasks' vindt u een overzicht van taken die nog moeten gebeuren. In alle views is het mogelijk om aan een pagina een taak te verbinden. Deze worden overzichtelijk gegroepeerd onder deze view.

Wanneer u met de rechter muisknop op een bestand klikt in één van de andere views, kan men een taak aanmaken.



Hier kan worden aangegeven:

- de naam van de taak;
- de prioriteit;
- de taak kan eventueel worden voorzien van enig commentaar.

Als er vervolgens op 'OK' wordt gedrukt, wordt de taak toegevoegd aan de view 'Tasks'

Figuur 20: nieuwe taak

Binnen de view 'Task' kan men met de rechter muisknop klikken op de taak. Men heeft vervolgens de keuze uit de volgende opties:

- **Edit Task**: als u hierop klikt, kunt u de gegevens van de taak wijzigen. Hetzelfde scherm als in Figuur 20 verschijnt.
- **Do Task**: bij het selecteren van deze optie wordt de FrontPage Editor opgestart, waarna de pagina waarbij de taak hoorde, kan worden bewerkt.
- **Mark Complete**: ongeacht of de taak is gedaan of niet, kan hier worden aangegeven dat de taak 'af' is.
- **Delete**: met deze keuze verwijdert u de taak.

Dit zijn de basisbeginselen van de FrontPage Explorer. Voor een uitgebreider handleiding wordt verwezen naar de helpfunctie die overal aanwezig is binnen de FrontPage Explorer.

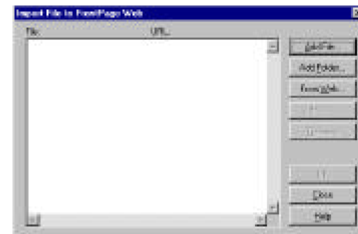
Oude website

Wanneer u reeds een andere ('oude') website hebt, kan deze geïmporteerd worden op de nieuwe kennisnetwebsite. Hiervoor moeten de volgende handelingen worden verricht.

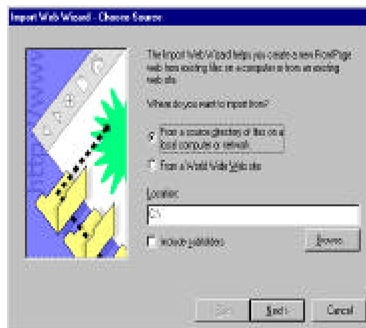
Open in FrontPage uw webserver bij kennisnet, zoals dat eerder in dit document staat beschreven. Klik op 'File' in het menu en klik vervolgens op 'Import…'. Er verschijnt een scherm zoals in Figuur 21.

Binnen dit scherm zijn er drie mogelijkheden.

- **Add File**: er kan een bestand worden ingevoegd.
- **Add Folder**: er kan een map worden ingevoegd.
- **From Web**: een bestaande website kan worden geïmporteerd op de kennisnetwebserver.



Figuur 21: importeren



Figuur 22: importeren: bron kiezen

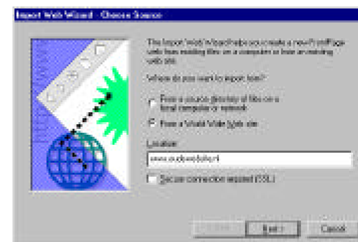
In dit voorbeeld wordt er vanuit gegaan dat er een bestaande website is die wordt geïmporteerd. Als er op de knop: 'From Web...' wordt gedrukt, verschijnt het volgende scherm (Figuur 22).

Er kan worden aangegeven of de pagina's zich op het lokale netwerk bevinden, of dat men al ergens een website heeft. Indien er al ergens een website bij een provider staat, kan op: 'From a World Wide Web site' worden geklikt.

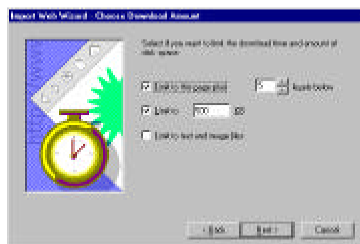
Staat de website ergens op het netwerk of de lokale harde schijf, dan kan er op: 'From a source directory or files on a local computer or network' worden geklikt.

In het volgende voorbeeld wordt er vanuit gegaan dat de website al ergens op Internet staat en dat er gekozen is voor de optie: 'From a World Wide Web site'. Het volgende scherm verschijnt (Figuur 23).

Hier kan de oude website worden geselecteerd en kan er worden aangegeven of de onderliggende mappenstructuur van de website wordt meegenomen. Dit doet men door op het aankruisvak 'Include subfolders' te klikken. Voer de naam van de te importeren website in bij 'Location'. Druk op 'Next>' om naar het volgende scherm te gaan.



Figuur 23: importeren: oude website



Figuur 24: importeren: 'diepte'

Binnen het volgende scherm kan worden opgegeven hoe 'diep' de oude website geïmporteerd moet worden. Dat wil zeggen: hoeveel niveaus van de bestandsstructuur (in hyperlinks) geïmporteerd dienen te worden. Waarschijnlijk zult u hier geen limiet aan willen stellen, wanneer u de *gehele* website wilt overnemen.

Ook kan worden opgegeven hoe groot (in kilobytes) in totaal de bestanden mogen zijn, die geïmporteerd gaan worden. Hier zult u eveneens geen limiet willen stellen wanneer u de *gehele* website wilt overnemen.

Tot slot kunt u aangeven dat alleen teksten en afbeeldingen (en niet bijvoorbeeld Java-applets, filmpjes en geluiden) geïmporteerd mogen worden.

Druk op 'Next>' om op het laatste scherm van de Import Web Wizard terecht te komen (Figuur 25).

Druk op Finish om de website te importeren. Hier kan enige tijd overheen gaan. Vooral als er veel plaatjes staan op de oude website, kan dit enige tijd duren. In de tussentijd ziet u het volgende scherm (Figuur 25).



Figuur 25: importeren: 'Finish'



Figuur 26: importstatus

Pagina's met dezelfde namen worden overschreven. Zodra de website is geïmporteerd, kan deze bewerkt worden op de gebruikelijk FrontPage-manier.

HULPMIDDELEN

Op het Internet zijn diverse hulpmiddelen te krijgen en is een schat aan informatie te vinden voor het maken van uw website. In deze paragraaf worden enkele interessante tips gegeven.

Informatiebronnen

- **Het Web Graphics Ontwerpboek** [1] Adres: http://www.lynda.com/.
- **Killersites**[2] Informatie voor webontwerpers. Adres: http://www.killersites.com.
- **Netscape Developer Site** De maker van het bladerprogramma 'Communicator' heeft op een speciale website een grote hoeveelheid informatie over het gebruik van onder andere HTML en JavaScript.
  Adres: http://developer.netscape.com/library/documentation/index.html.

On line hulpmiddelen

Er bestaan enkele interessante websites die u op weg kunnen helpen met het maken van een goede en mooie website. Hier volgt een rijtje van handige websites.

- **Bryan Livingston's CoolText.com: Online Graphics Generator.** Dit is een gratis dienst waar u kleine plaatjes kunt laten genereren, zoals knopjes, paginakoppen en achtergronden. Voor het maken van deze plaatjes wordt, via een webinterface, gebruikgemaakt van de eveneens gratis software GIMP. Adres: http://www.cooltext.com/.

[1] Bron: Automatisering Gids, Ten Hagen Stam uitgevers, 's-Gravenhage, vrijdag 12 februari 1999 - nr. 6, bladzijde 17.

[2] Bron: Automatisering Gids, Ten Hagen Stam uitgevers, 's-Gravenhage, vrijdag 12 februari 1999 - nr. 6, bladzijde 17

Software

- **GNU Image Manipulation Program.** Kortweg 'GIMP' – een handig en krachtig tekenprogramma voor UNIX-systemen, waaronder Linux, en het is gratis te gebruiken onder de voorwaarden van de GNU General Public Licence. Adres: http://www.gimp.org/.
- **The Free Builder Project.** 'Free Builder' is een gratis ontwikkelgereedschap voor Java^{tm}. Er zijn distributies beschikbaar voor Windows en UNIX-systemen.
- **Tucows.** Op de websites van Tucows kunt u voor o.a. Windows, MacOS en Java verschillende hulpmiddelen vinden voor het maken en onderhouden van HTML-pagina's.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonische te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen aan 'handboek@kennisnet.nl'.

Index

Figurenlijst

Literatuur

- Telemark Systems, Inc.; "NT DNS Configuration - using BIND 4.9.3 Release"; Telemark Systems, Inc., april 1996; http://www.telemark.net/~randallg/ntdns.htm.
- Langfeldt, Nicolai <janl@math.uio.no>; "DNS-HOWTO" (Linux HowTo); Langfeldt, Nicolai, 1995-1999; http://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

Datum : 15 juni 2000
Versie : 20000615.01

Documentnr.: 995047

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel V, Geavanceerde instellingen

Indeling van dit document

Bepaalde scholen, met name die reeds enige ervaring met het Internet hebben opgebouwd, hebben nogal eens wat vragen en wensen rond het aansluiten van hun eigen apparatuur en voorzieningen. Getracht wordt in dit deel hierop een antwoord te geven.

In Hoofdstuk 1 wordt uitgelegd hoe u een eigen DHCP-server kunt opzetten.

Hoofdstuk 2 gaat in op zaken rond een eigen DNS-server.

In Hoofdstuk 3 wordt uitleg gegeven over het opzetten van een eigen proxyserver.

Hoofdstuk 4 gaat in op de vraag hoe u een eigen mailserver kunt inrichten.

Hoofdstuk 5 behandelt het onderwerp 'Een eigen webserver'.

Hoofdstuk 6 behandelt vragen rond de IP-adressering op kennisnet en adresvertaling (Network Address Translation, NAT).

In Hoofdstuk 7 worden vragen over netwerkkoppelingen behandeld.

Inhoudsopgave

Hoofdstuk 1. Een eigen DHCP-server

1.1 Kan ik zelf een DHCP- of BOOTP-server opzetten?

Dat kan, mits u de aan u verstrekte IP-adressen voor kennisnet gebruikt en hiertoe via het Servicepunt kennisnet een verzoek indient. De voor u beschikbaar gestelde reeks IP-adressen zal uit de centrale DHCP-server worden verwijderd en DHCP-relay zal op de router worden uitgeschakeld. Vervolgens kunt u uw eigen DHCP- en/of BOOTP-server starten.

Enkele gegevens die u nodig hebt:

Default gateway	het IP-adres van uw router
DNS-servers	212.178.5.4 en 212.178.5.5

De volgende subparagrafen beschrijven de configuratie van DHCP-servers. Hierbij wordt echter gebruikgemaakt van een fictieve reeks IP-adressen.

1.1.1 Microsoft DHCP-server

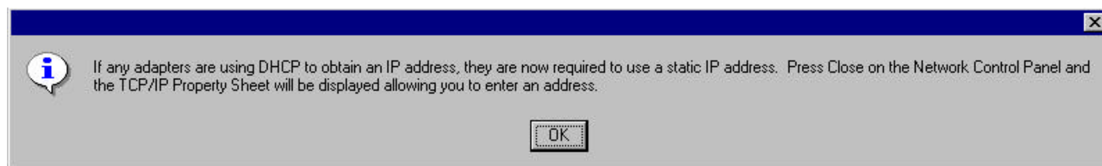
De Microsoft DHCP-server is een optioneel onderdeel van Windows NT-server. Mogelijk dient u dit nog te installeren.

Open het venster met instellingen, kies dan netwerk ('Network') en ga naar het tabblad 'Services'. Controleer of de DHCP-server in het rijtje voorkomt.

Indien dit niet het geval is, klikt u op 'Toevoegen' of 'Add...'. U krijgt een venster te zien, waarin u de DHCP-server dient te selecteren. U zult waarschijnlijk worden gevraagd om de CD-ROM te plaatsen voordat u de installatie kunt voltooien.

Figuur 1: installatie NT Network Services

Figuur 2: te installeren services



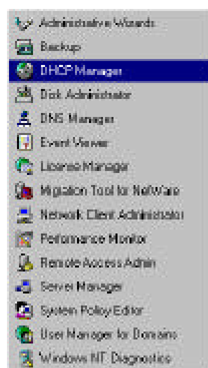
Figuur 3: waarschuwing bij installatie DHCP-server

Bij de installatie van de DHCP-server krijgt u waarschijnlijk een waarschuwing dat de NT-server zelf een statisch adres dient te krijgen voordat op deze machine de DHCP-server kan worden gestart.

Klik op ‘OK’ om de installatie te voltooien. Sluit de configuratieschermen. U dient nu de computer te herstarten.



Figuur 4: Reboot na installatie



Figuur 5: administratieve hulpmiddelen

Na de herstart van de computer dient de DHCP-server geconfigureerd te worden. Klik op de Start-knop voor het menu en ga naar de 'Administrative Tools', ofwel de 'Beheerhulpmiddelen'.

Uit dit menu opent u de ‘DHCP Manager’.

In het venster dat verschijnt, staat één object: de lokale server. Selecteer dit object en kies uit het menu de optie 'Create Scope'.

Er verschijnt een venster waarin u een 'Scope' kunt aanmaken. Hiermee definieert u de uit te delen IP-adressen en aanverwante gegevens.

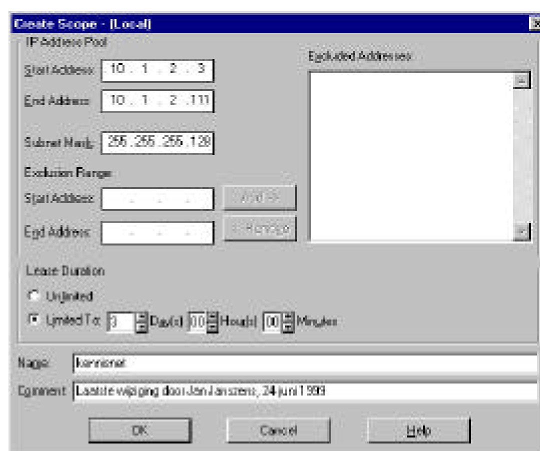
U begint door het eerste en laatste adres uit de IP-reeks op te geven. Vervolgens kunt u het netwerkmasker opgeven. In het voorbeeld is een reeks van in totaal 128 adressen, met netwerkmasker '`255.255.255.128`' gebruikt. Er worden echter slechts 103 adressen voor werkstations uitgedeeld.

Let op dat de start- en eindadressen binnen dezelfde reeks, welke mede wordt bepaald door het netwerkmasker, vallen!

Analoog aan de reeks kunt u een aantal subreeksen uitsluiten, bijvoorbeeld omdat u enkele statische adressen aan werkstations wilt uitdelen. Deze reeksen komen in het vak rechts te staan.

Onder de IP-gegevens kunt u de geldigheidsduur van de uitgedeelde IP-adressen aangeven. Standaard is dit drie dagen. Wanneer er weinig verandering in uw netwerk plaatsvindt, is dit een goede waarde, maar wanneer u veel denkt te veranderen of regelmatig 'bezoekers' hebt, kunt u deze tijd beter korter instellen.

U kunt bijna onderaan een naam opgeven voor de reeks. Een voor de hand liggende keuze is 'kennisnet'. Tevens kunt u nog een omschrijving van één regel opgeven voor de scope.



Figuur 6: Scope aanmaken

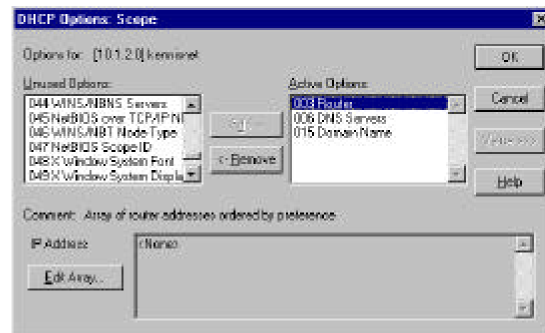


Figuur 7: Scope activeren?

Na het aanmaken van de scope zal worden gevraagd of u deze ook wilt activeren. Het verdient aanbeveling om hier negatief te antwoorden en de scope pas te activeren wanneer u klaar bent met de configuratie van de gegevens.

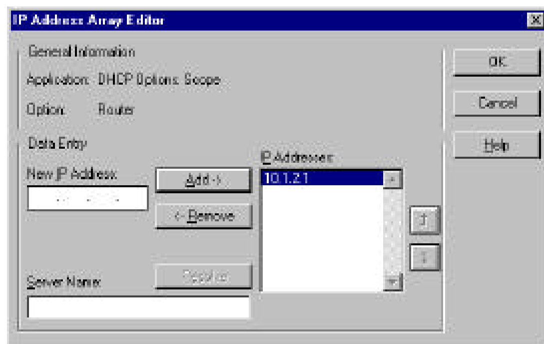
Selecteer de lokale scope wederom en kies uit het menu 'Options' voor 'Scope'. Er verschijnt een venster waarin u nog enkele gegevens voor de scope kunt toevoegen voor wat betreft de uit te delen informatie.

Het wordt aangeraden om uit de linker lijst ten minste de 'Router', de 'DNS Servers' en 'Domain Name' in de rechter lijst op te nemen. Mogelijk hebt u nog behoefte om bijvoorbeeld een eigen WINS-server op te zetten en deze als DHCP-optie mee te geven.



Figuur 8: opties voor de scope

U kunt nu alle opties configureren door deze te selecteren. Klik op de knop 'Value>>>' om de bijbehorende gegevens in te kunnen vullen.



Figuur 9: router voor een scope

Met de knop 'Edit Array...' kunt u voor de optie 'Router' de gegevens wijzigen.

Normaliter is er slechts één gateway in uw lokale netwerk. Vul het IP-adres hiervan in (zie eventueel bijlage A om te bepalen wat het adres van uw router is) onder 'New IP Address:'/'Nieuw IP-adres:' en voeg het toe aan de lijst.

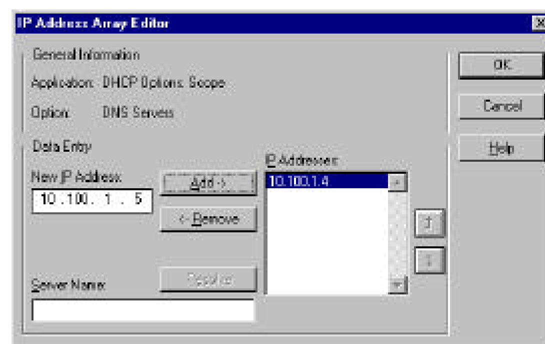
Het routeradres dient uiteraard binnen hetzelfde subnet te vallen als de uit te delen IP-adressen en niet te overlappen met de reeks uit te delen IP-adressen.

Klik op 'OK' om dit venster te sluiten.

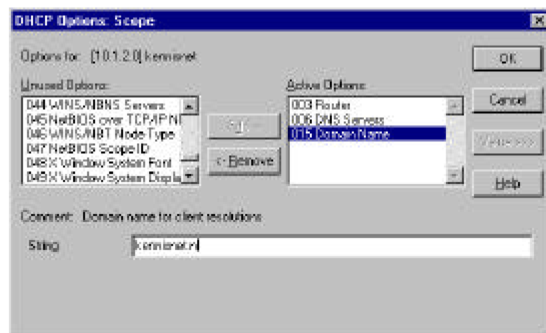
Met de knop 'Edit Array...' kunt u voor de optie 'DNS Servers' de lijst van servers wijzigen. Typ in het venster dat verschijnt onder 'New IP Address:' de IP-adressen van de DNS-servers van kennisnet en klik op 'Add->'. Indien u lokaal een 'Caching DNS Server' hebt, dient u mogelijk dit adres in te geven.

De DNS-servers van kennisnet zijn:

- 212.178.5.4
- 212.178.5.5



Figuur 10: DNS-servers voor een scope



In het optievenster zelf kunt u door de optie 'Domain Name' (of 'Domeinnaam') te selecteren de domeinnaam opgeven, namelijk 'kennisnet.nl'.

Sluit vervolgens het venster met 'OK'.

Activeer eventueel de scope via het menu en sluit de DHCP-manager.

U dient nu eventueel nog de service te activeren.

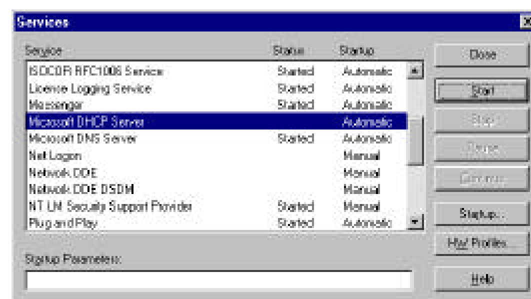
Figuur 11: domeinnaam voor een scope



Figuur 12: Windows NT Services

Open het configuratiescherm voor de 'Services' en selecteer de 'Microsoft DHCP Server'. Controleer de ‘Status’ en 'Startup'. Indien de status 'Started' is, is de service reeds actief. Anders dient u deze alsnog te starten met 'Start', rechts in het venster.

De vermelding onder 'Startup' dient 'Automatic'/'Automatisch' te luiden. Dit kunt u eventueel aanpassen met de knop 'Startup...'.



Figuur 13: configuratiescherm Services

1.1.2 ISC DHCP-server

De DHCP-server van The Internet Software Consortium (ISC: http://www.isc.org/) kan worden gebruikt op de meest gangbare UNIX-achtige platforms, waaronder:

- SunOS/Solaris;
- MacOS X;
- Linux;
- FreeBSD;
- NetBSD.

Voor een volledige lijst kunt u kijken op de bovengenoemde website. Kijk hiervoor bij versie 2; versie 1 is verouderd en versie 3 is nog sterk in ontwikkeling!

Bij RedHat Linux wordt deze DHCP-server in de distributie op CD-ROM meegeleverd en kan 'on the fly' geïnstalleerd worden via de Package Manager. Dit gaat zoals hieronder beschreven. Voor andere systemen zult u dit mogelijk 'met de hand' moeten doen volgens de instructies in het pakket dat u bij ISC kunt ophalen.

1.1.2.1 Installatie bij RedHat Linux

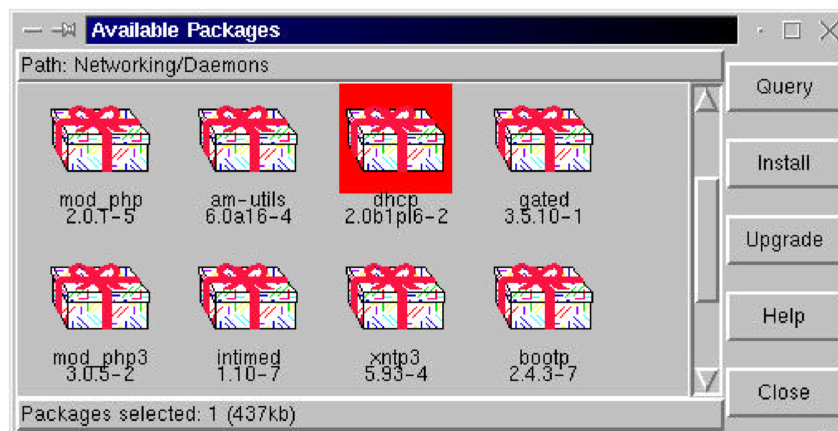
Open het Control Panel van RedHat Linux (bij een standaardinstallatie start dit voor 'root' altijd direct op in een X-sessie). En selecteer de Package Manager.

Klik dan op de knop 'Available'. Het onderstaande venster verschijnt, tenminste wanneer de RPM-bestanden (op de CD-ROM) te vinden zijn. Ga naar 'Networking' en dan 'Daemons'. Hier staat als het goed is het pakket `dhcp<versie>`. Selecteer het pakket en klik op 'Upgrade' of 'Install' om het te installeren.

De volgende stap is om de DHCP-server te configureren. De service is reeds in de opstartscripts van het systeem verwerkt. Een Reboot is echter niet nodig, zoals zal blijken.



Figuur 14: Control Panel



Figuur 15: Package Manager, Networking/Daemons

1.1.2.2 Configuratie

In `/etc/dhcpd.conf` is de configuratie voor de DHCP-server opgenomen. Deze dient u uiteraard aan uw lokale situatie aan te passen. Hieronder is een basisconfiguratie gegeven. De in rood weergegeven teksten dient u (mogelijk) te vervangen voor uw eigen situatie.

Regels die beginnen met een hekje (#) zijn commentaar. Alle andere regels dienen door een puntkomma (;) te worden afgesloten. Raadpleeg de bij de server behorende documentatie voor meer informatie (UNIX-commando: `man dhcpd.conf`).

```
# dhcpd.conf
#
# Configuratiebestand voor ISC dhcpd
#

# Machines met meerdere netwerkinterface dienen een 'serveridentificatie'
# ('server-identifier') op te geven. Dit dient het primaire IP-adres van
# de machine te zijn, of tenminste een adres dat niet snel zal veranderen

server-identifier 10.1.2.112;
```

```
# hier volgen opties voor alle ondersteunde netwerken...

option domain-name "kennisnet.nl";
option domain-name-servers 212.178.5.4, 212.178.5.5;

# Een 'shared-network' is bedoeld om netwerkreeksen met dezelfde fysieke
# interface te groeperen. De naam 'SCHOOL' is slechts een voorbeeld en
# kan willekeurig worden opgegeven. Gebruik uitsluitend letters en cijfers.

shared-network SCHOOL {

# hier volgen opties voor alle systemen binnen dit 'shared-network'
  option subnet-mask 255.255.255.128;
  # 1 dag (86400 seconden)
  default-lease-time 86400;
  # 3 dagen
  max-lease-time 259200;

# Deze school heeft slechts één IP-reeks van 128 adressen. Dit wordt
# aangegeven met de opdracht 'subnet' en de bijbehorende gegevens.
# Dit is te vergelijken met een 'Scope' in de NT-configuratie.
# Opties in dit blok kunnen tussen de accolades ('{' en '}') worden
# opgegeven en overschrijven de algemene opties voor het 'shared-network'

  subnet 10.1.2.0 netmask 255.255.255.128 {
    # Geef met 'range <begin> <eind>' aan welke subreeks adressen u
    # wilt uitdelen. Dit kunnen meerdere subreeksen binnen de totale
    # IP-reeks zijn. Dit doet u door meerdere keren de opdracht 'range'
    # te geven.
    range 10.1.2.3 10.1.2.111;
    option broadcast-address 10.1.2.127;
    option routers 10.1.2.1;
  }
}
```

Via de webpagina http://enbvlists.kennisnet.nl/techniek/ kunt u, op basis van de aan u uitgedeelde IP-gegevens, een dergelijke DHCP-configuratie laten construeren. Op de website http://members.xoom.com/vschade/dhcp-conf/ vindt u een hulpmiddel om een DHCP-configuratie te maken en te beheren.

1.1.2.3 Opstarten

U start de server door het betreffende opstartscript aan te roepen of, indien u de server handmatig hebt geïnstalleerd, door het programma zelf te starten, eventueel met extra parameters.

Bij RedHat Linux:

```
/etc/rc.d/init.d/dhcp start
```

Via de runlevel editor van RedHat Linux (in het Control Panel) kunt u de DHCP-servers toevoegen aan de gewenste runlevels[1], bijvoorbeeld: 3 tot en met 5.

'Met de hand':

```
/usr/sbin/dhcpd
```

(Aangenomen is dat de server in de map /usr/sbin is geïnstalleerd; dit kan per systeemimplementatie verschillen.)

[1] Een runlevel is een bepaalde stand van het systeem.

Hoofdstuk 2. Een eigen DNS-server

Dit hoofdstuk behandelt het opzetten van een eigen DNS-server ten behoeve van het lokale netwerk.

Belangrijk is op te merken dat, wanneer u zelf een DNS-server opzet, u het beste ook een eigen DHCP-server kunt opzetten. U kunt op die manier namelijk aan uw werkstations doorgeven dat deze van uw eigen DNS-server gebruik dienen te maken.

2.1 Hoe kan ik een eigen DNS-server opzetten?

U dient gebruik te maken van de DNS-servers van kennisnet als zogenaamde 'parent' of 'forwarder' (dit zijn twee namen voor hetzelfde). Hoe u dit precies doet, is afhankelijk van het gebruikte product. Veruit het meest gebruikte product is 'BIND' van het 'Internet Software Consortium' (`http://www.isc.org/`). Veel andere producten zijn gebaseerd op BIND. In deze paragraaf wordt voor een aantal producten uitgelegd hoe u deze kunt configureren.

Indien u gebruik wilt maken van uw eigen DNS-server, dan wordt het aangeraden om tevens een eigen DHCP-server op te zetten, waarbij u de correcte IP-adressen voor de DNS-servers opgeeft. Een andere optie is om wel gebruik te maken van de centrale DHCP-service, maar in alle systemen uitsluitend de DNS-servers statisch te configureren.

U dient de DNS-server voor uw lokale netwerk in de niet-afgeschermde reeks te plaatsen (zie bijlage A.), zodat deze kan communiceren met de centrale DNS-servers van kennisnet.

2.1.1 BIND (UNIX)

Voor (vrijwel) elk Unix-achtig besturingssysteem is BIND verkrijgbaar. Bij de meeste Linux-distributies wordt het standaard meegeleverd. Voor installatie: zie ook paragraaf 1.1.2.1, of de installatiehandleiding van uw besturingssysteem. U kunt ook een broncodedistributie ophalen bij `http://www.ics.org/`.

Er zijn grofweg twee 'smaken': versie 4.x en versie 8.x. In dit geval wordt uitsluitend versie 8 besproken. Het belangrijkste bestand is '`/etc/named.conf`', dat de basis van de configuratie vormt en aangeeft voor welke 'zones' de nameserver verantwoordelijk is. Alle regels die beginnen met '//' vormen commentaar.

```
// Globale opties voor de DNS-server
options {
        // alle overige bestanden staan in /var/named
        directory "/var/named";
        // gebruikt 'forwarders' voor onbekende gegevens
        forward first;
        forwarders {
          212.178.5.4;
          212.178.5.5;
        };
};

//
// Configuratie voor een 'caching only nameserver'
// (uitgeschakeld)
//zone "." {
//        type hint;
//        file "named.ca";
//};
```

```
//
// Configuratie voor de 'reverse zone' voor 127.0.0.x
//
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

In de bovenstaande configuratie is de 'caching only'-functie uitgeschakeld. Deze functie zorgt ervoor dat, wanneer onbekend is wat het antwoord op een gestelde vraag is, opgezocht kan worden waar het antwoord wel kan worden verkregen. Hiervoor wordt een lijst met de 'root name servers' (ftp://ftp.rs.internic.net/domain/named.root) gebruikt. Binnen kennisnet heeft het gebruik hiervan geen zin, daar deze servers niet bereikbaar zijn en daarom worden 'forwarders' gebruikt.

Er is echter wel een 'zone' "0.0.127.in-addr.arpa" aangemaakt. Deze zone is noodzakelijk voor het opzoeken van het 'loopback'-adres[2]: 127.0.0.1. Zoals aangegeven in het configuratiebestand is deze zone in het bestand `/var/named/named.local`. Het bestand ziet er als volgt uit:

```
@       IN      SOA     localhost. root.localhost.  (
                              1997022700 ; Serial
                              28800      ; Refresh
                              14400      ; Retry
                              3600000    ; Expire
                              86400 )    ; Minimum
        IN      NS      localhost.

1       IN      PTR     localhost.
```

Meestal wordt dit bestand, mogelijk met een andere naam, standaard meegeleverd met BIND.

Start BIND en u kunt gebruikmaken van de nameserver. Hoe u BIND precies start, is afhankelijk van uw systeem. U kunt in ieder geval het programma zelf (zonder 'nette' opstartscripts te gebruiken) opstarten met `/usr/sbin/named` (mogelijk is het pad afwijkend op specifieke systemen; raadpleeg de bijgevoegde documentatie voor uw systeem).

Onder RedHat Linux kunt u, mits u de standaardinstallatie gebruikt hebt, de service starten met het commando '`/etc/rc.d/init.d/named start`'.

Optioneel kunt u zelf zones toevoegen aan uw configuratie. Voor meer informatie over het opzetten van een DNS kunt u ook de Linux-HOWTO raadplegen:

ftp://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

2.1.2 BIND (Windows NT)

BIND voor Windows NT is een afgeleide van de Unix-versie van BIND. Het is gebaseerd op versie 4.9.3. Daardoor is het hoofdconfiguratiebestand anders.

Het configuratiebestand (`named.boot` of `named.ini`) dient u te plaatsen in de Windows-directory (meestal `C:\WINNT`). Alle regels die beginnen met een puntkomma, worden als commentaar beschouwd. Een bestand analoog aan dat voor versie 8.x voor Unix ziet er ongeveer als volgt uit:

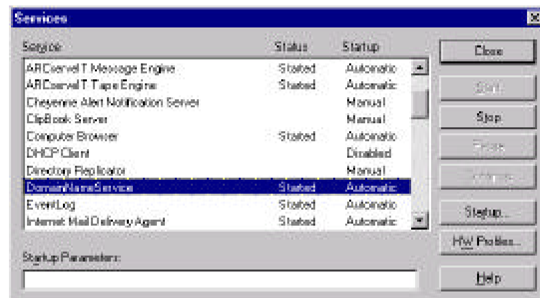
[2] De bijbehorende naam is 'localhost'. Dit adres wordt gebruikt om een machine in ieder geval met zichzelf te kunnen laten verbinden. Bijvoorbeeld een commando als 'ping localhost' (Onder Unix, OS/2 of Windows) zal altijd antwoord moeten geven.

```
directory \\var\\named

; cache   .        db.cache

primary 0.0.127.IN-ADDR.ARPA    named.local
forwarders    212.178.5.4 212.178.5.5
```

De overigen bestanden bevinden zich (in dit voorbeeld) in `C:\VAR\NAMED` (onder Windows NT is er geen onderscheid tussen hoofd- en kleine letters). Let op de dubbele 'backslash' (\)! Het bestand 'named.local' is identiek aan dat wat voor de Unix-versie 8.x wordt gebruikt.



Figuur 16: Windows NT Service: DomainNameService

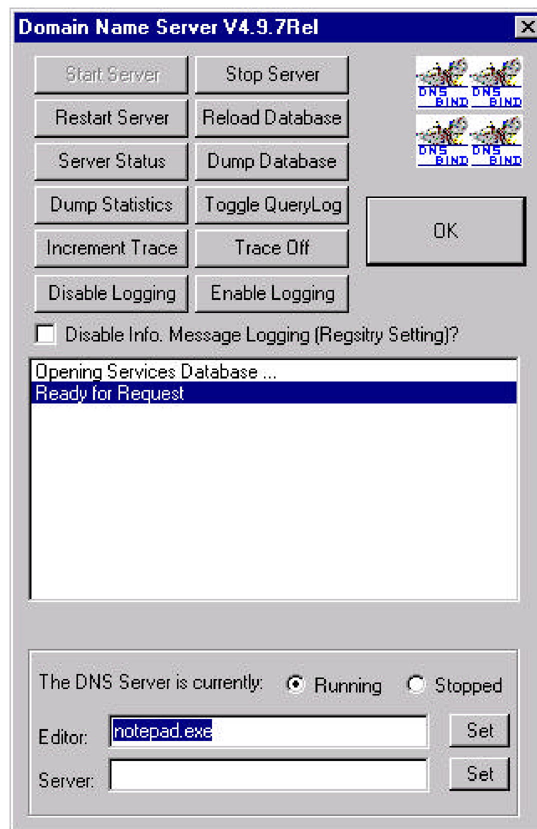
U kunt de server starten en stoppen via de 'Services' van Windows NT. Open het configuratiescherm. Dubbelklik 'Services' en selecteer 'DomainNameService'. Met de knoppen 'Start' en 'Stop' kunt u de service bedienen. Om de service automatisch te laten opstarten bij het starten van het systeem, klikt u op 'Startup...' c.q. 'Opstarten' en selecteert u 'Automatic' of 'Automatisch'.

Zorg ervoor dat er geen andere DNS-server, bijvoorbeeld de Microsoft DNS-Server, actief is wanneer u BIND-NT activeert!

De DNS-service heeft ook een eigen Control Panel: de BIND NT DNS Controller, welke zich eveneens in het configuratiescherm bevindt.

In dit scherm kunt u ook de server starten en stoppen, maar ook een actieve server dwingen om de gegevens opnieuw in te lezen ('Reload Database').

Tevens kunt u in dit scherm logbestanden van de DNS-server aan- en uitzetten en bekijken.

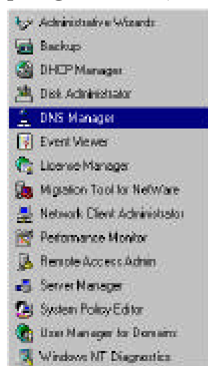


Figuur 17: BIND-NT Controller

U kunt BIND-NT ophalen op `http://www.software.com/scripts/reg-bind.pl`. Meer informatie over BIND-NT vindt u op `http://www.telemark.net/~randallg/ntdns.htm`. Deze pagina bevat aanwijzingen over installatie en configuratie van de software.

2.1.3 Microsoft DNS Server (Windows NT)

Een alternatief voor BIND-NT is de eigen DNS-server van Microsoft, welke bij Windows NT-server wordt meegeleverd. De installatie hiervan gaat analoog aan de installatie van de DHCP-server (zie paragraaf 1.1.1).

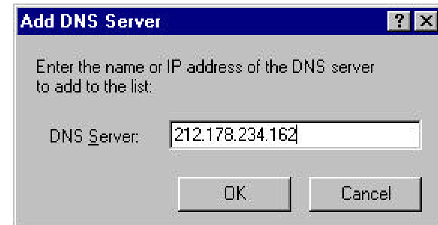


Figuur 18: administratieve hulpmiddelen

Na de herstart van de computer dient de DNS-server geconfigureerd te worden. Klik op de Start-knop voor het menu en ga naar de 'Administrative Tools', ofwel de 'Beheerhulpmiddelen'. Uit dit menu opent u de DNS Manager.

Als het de eerste keer is dat u de DNS Manager opstart, staat er uitsluitend een icoontje van de 'Server List'. Klik met de rechter muisknop op de 'Server List' en kies 'Add DNS Server' (of het equivalent in het Nederlands).

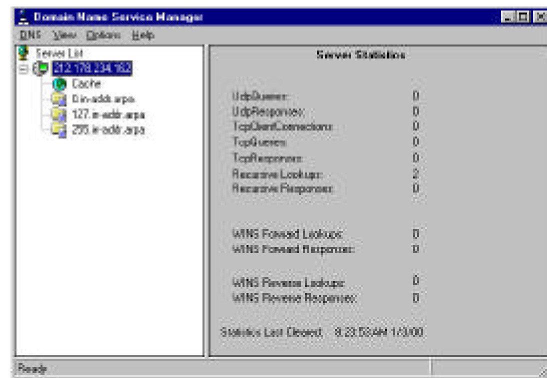
Typ in het venster dat dan verschijnt het IP-adres of de DNS-naam van de server die u toe wilt voegen. Klik vervolgens op ‘OK’.



Figuur 19: voeg een DNS-server toe

Er wordt een servericoontje aangemaakt. Dubbelklik op het icoontje om het uit te vouwen. Er verschijnt een lijstje met de 'Cache' en een aantal voorgedefinieerde zones.

Klik nu met de rechter muisknop op de zojuist aangemaakte server en kies 'Properties' (of 'Eigenschappen'). Er verschijnt een klein venster met een drietal tabbladen.

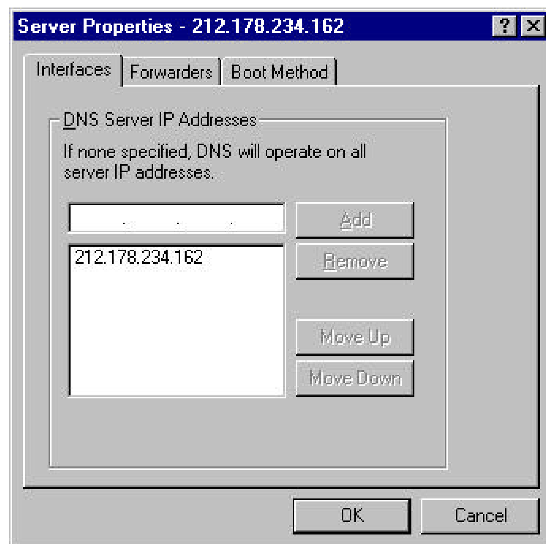


Figuur 20: DNS-servers

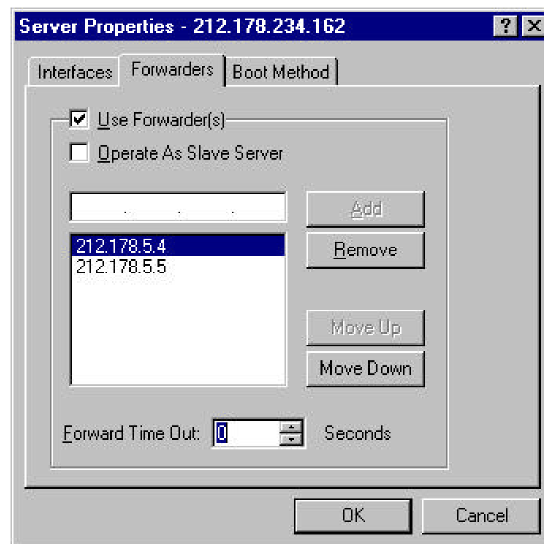
Op het eerste tabblad (Figuur 21) kunt u aangeven op welke interfaces de DNS-server moet 'luisteren'. Dit zijn de IP-adressen van de netwerkkaarten, indien er meerdere zijn. Meestal zult u de standaardinstellingen kunnen gebruiken.

Op het tabblad 'Forwarders' (Figuur 22) kunt u de IP-adressen van de 'forwarding DNS-servers', in dit geval de centrale DNS-servers van kennisnet, aangeven. Vink het vakje 'Use Forwarder(s)' aan en vul de IP-adressen (212.178.5.4 en 212.178.5.5) in.

U kunt ervoor kiezen om ook 'Operate As Slave Server' aan te vinken. Dit zorgt ervoor dat *alle* verzoeken worden doorgestuurd en er niet naar lokale zones/domeinen wordt gekeken.



Figuur 21: MS DNS Server: eigenschappen, interfaces



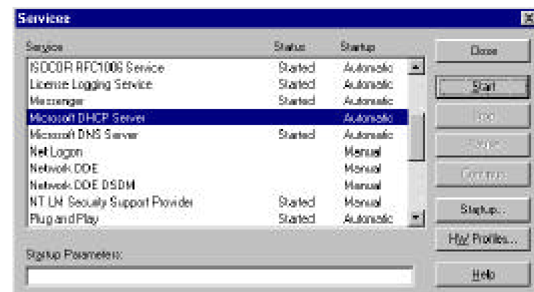
Figuur 22: MS DNS Server: eigenschappen, forwarders



Figuur 23: Windows NT Services

Open het configuratiescherm voor de 'Services' en selecteer de 'Microsoft DNS Server'. Controleer de ‘Status’ en 'Startup'. Indien de status 'Started' is, is de service reeds actief. Anders dient u deze alsnog te starten met 'Start', rechts in het venster.

De vermelding onder 'Startup' dient 'Automatic'/'Automatisch' te luiden. Dit kunt u eventueel aanpassen met de knop 'Startup...'.

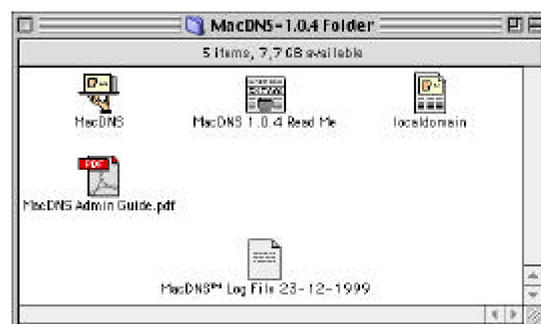


Figuur 24: configuratiescherm Services

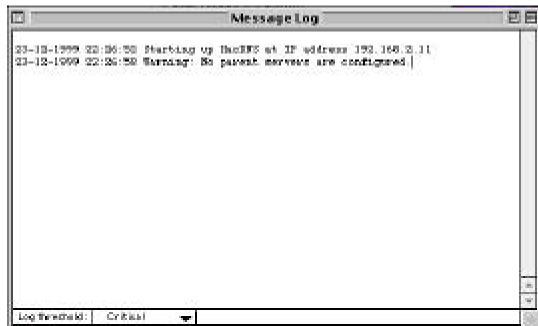
2.1.4 MacDNS

Voor de Apple Macintosh kunt u MacDNS gebruiken om een eigen DNS-server op te zetten. MacDNS is helaas niet zo uitgebreid als BIND of de Microsoft DNS-server, maar is redelijk eenvoudig te bedienen. Volg bij het installeren de aanwijzingen die in het begeleidende tekstbestand staan ('MacDNS <*versie*> Read Me'). Zo dient u een 'alias' van het programma in de opstartmap te plaatsen om MacDNS automatisch te starten bij het opstarten van het systeem.

Om MacDNS te configureren, gaat u als volgt te werk.



Figuur 25: map MacDNS



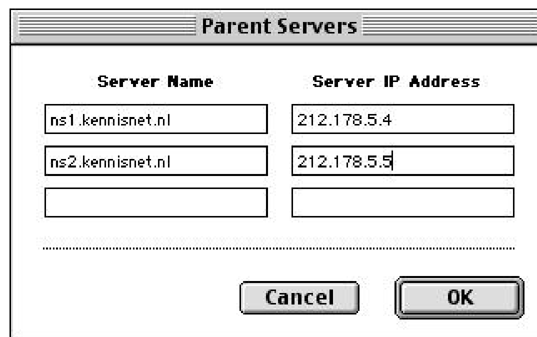
Figuur 26: MacDNS: Message Log

Start MacDNS. U krijgt, als het goed is, het venster met de logs te zien. Hier staan alle wijzigingen die u uitvoert, informatie over gebeurtenissen, foutmeldingen, etc.

Kies uit het menu 'Hosts' de optie 'Set Parent Servers'. In het scherm dat nu verschijnt, kunt u een maximum van drie 'parents' opgeven. Links dient u de naam van de server in te vullen en rechts het bijbehorende IP-adres. Voor kennisnet vult u in:

- '`ns1.kennisnet.nl`' met adres `212.178.5.4`
- '`ns2.kennisnet.nl`' met adres `212.178.5.5`.

Wanneer u geen eigen domein wilt aanmaken, dan bent u nu in principe klaar.



Figuur 27: MacDNS: Parent Servers

Figuur 28: MacDNS: Zone Information

Om zelf een domein toe te voegen, toetst u Command-N ('Appeltje-N') in. Het 'Zone Information'-scherm verschijnt. U kunt hier de domeinnaam, de eerste en eventueel de tweede nameserver en het e-mailadres van de beheerder (‘Administrator’) opgeven. Tevens kunt u enkele periodes opgeven.

- **Refresh Interval:** de tijd die moet verstrijken voordat een 'secondary' (kopie) nameserver controleert of er weer nieuwe informatie over de zone beschikbaar is.
- **Retry Interval:** de tijd die verstrijkt voordat de secondary nameserver, na een mislukte poging de zone over te halen, dit opnieuw probeert.
- **Expire Interval:** de tijd waarna een secondary nameserver de opgeslagen gegevens *moet* verwijderen.
- **Minimum TTL:** de periode waarin gegevens over een host opgeslagen mogen worden in de buffers van een andere DNS-server.

Met het scherm 'Host Information' (Command-H) kunt u een host toevoegen. U dient ten minste de betreffende nameserver toe te voegen. De naam die u achter 'Host Name' invult, dient ten minste de domeinnaam te bevatten. Het IP-adres is verplicht om in te vullen.

De 'Time to Live' is hetzelfde als 'Minimum TTL' voor een zone, maar dan specifiek voor één machine.

Achter 'Aliases:' kunt u, door komma's gescheiden, eventuele aanvullende namen voor dezelfde machine opgeven. Achter 'Mail Exchangers:' vult u, eveneens door komma's gescheiden, een prioriteit (getal) en een volledige machinenaam (eindigend meet een punt!) voor de mailserver voor deze machine op. De prioriteit is een numerieke waarde: hoe lager het getal, hoe hoger de prioriteit, ofwel hoe eerder deze benaderd zal worden om de mail te bezorgen.

Figuur 29: MacDNS: Host Information

Figuur 30: MacDNS: MX-Only Host Information

Het is ook mogelijk om alleen een 'Mail Exchanger' voor een (sub)domein op te geven, zonder dat er een IP-adres aan wordt gekoppeld. Om voor de zone zelf een 'Mail Exchanger' aan te geven, dient u geen machinenaam op te geven bij 'Host Name:', maar uitsluitend het domein!

Achter 'Mail Exchangers:' vult u de prioriteiten en de volledige namen van de mailservers in.

Hoofdstuk 3. Een eigen proxyserver

3.1 Kan ik mijn eigen webproxy blijven gebruiken?

Ja, mits deze ondersteuning biedt voor het Internet Caching Protocol (ICP) of Caching Array Routing Protocol (CARP) voor web. Met één van deze protocollen kan uw eigen webproxy als 'slave' van de proxyserver in het serverpark fungeren.

3.2 Hoe kan ik mijn eigen proxyserver aan de proxyserver van kennisnet koppelen?

U dient uw proxyserver zo te configureren dat deze op zijn beurt gebruikmaakt van de proxyserver in het serverpark (proxy.kennisnet.nl) via ICP of via CARP. Hoe dit precies werkt is afhankelijk van de gebruikte software.

Open het configuratiescherm van uw proxyserver en geef de kennisnetproxies op als 'ouder' ('parent') van uw proxy. Voor ICP dient u poort 3130 van `proxy.kennisnet.nl` op te geven; voor CARP dient u poort 8080 van `proxy.kennisnet.nl` op te geven.

Meer informatie kunt u (onder andere) vinden op de volgende adressen:

- http://www.microsoft.com/proxy/documents/CarpWP.exe
- http://cgi.netscape.com/proxy/v3.5/index.html
- http://developer.netscape.com/docs/manuals/proxy.html
- http://www.csm-usa.com/proxy/admin/carp/
- http://cache.is.co.za/squid/

3.2.1 CSM Proxy

Voor de CSM-proxy is een redelijk uitgebreid, Engelstalig handboek te vinden, op de website van CSM. Op het onderstaande adres vindt u de uitleg over het instellen van CARP.

http://www.csm-usa.com/proxy/admin/carp/.

U dient als 'parent' '`proxy.kennisnet.nl`', of apart '`proxy1.kennisnet.nl`' én '`proxy2.kennisnet.nl`' op te geven.

3.2.2 Netscape Proxy

Netscape heeft een grote verzameling on line handboeken van de verschillende producten. Hier kunt u de handleidingen vinden voor zowel de Windows NT-versie als de UNIX-versie van de Netscape Proxy. Het adres voor de proxyhandleidingen is:

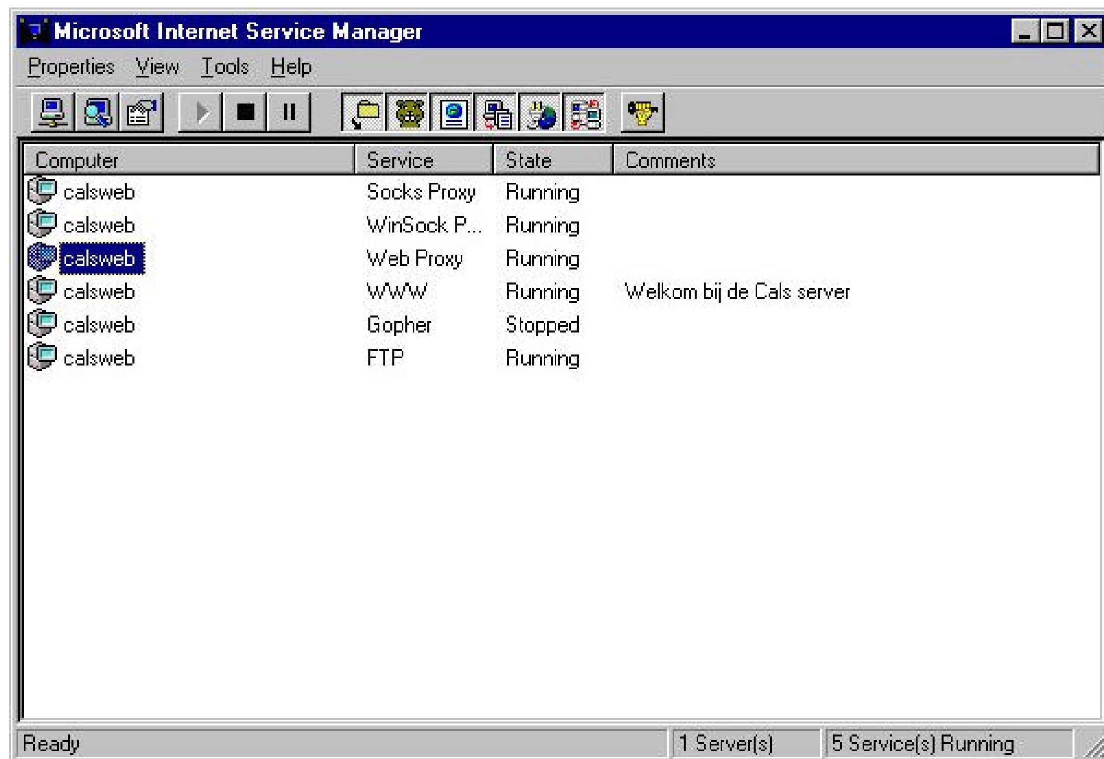
http://developer.netscape.com/docs/manuals/proxy.html.

3.2.3 Microsoft Proxy[3]

Het is mogelijk om met de Microsoft Proxy (voor Windows NT) een relatie met de centrale kennisnet-proxies te definiëren en zo uw eigen netwerk lokaal proxyfunctionaliteit te bieden. Hiertoe dient u als volgt te werk te gaan.

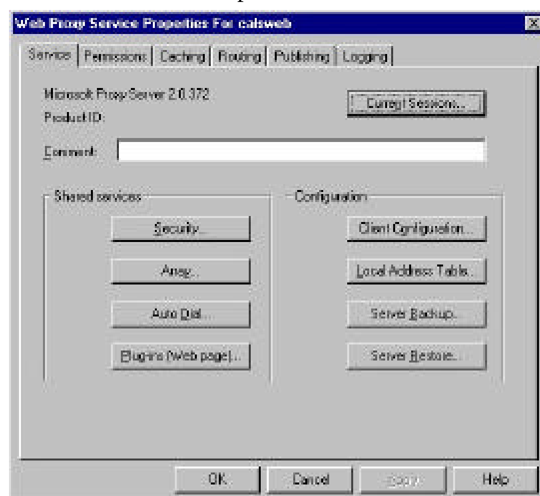
Start de Internet Service Manager.

[3] Met dank aan Harry Spek, ICT-coördinator Calscollege Nieuwegein.

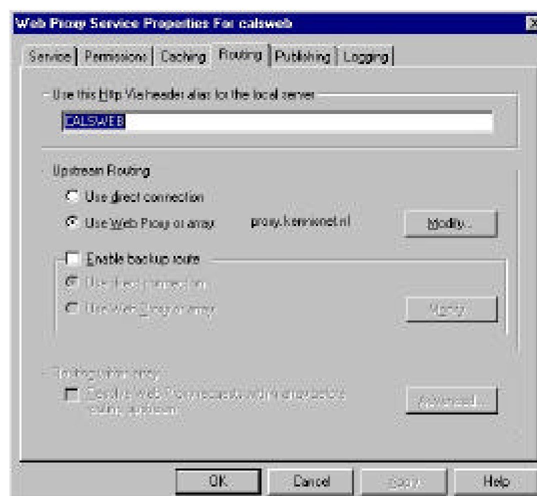


Figuur 31: Internet Service Manager

Verifieer dat de webproxy actief is. Indien dat het geval is, staat in de kolom 'State' de vermelding 'Running'. Dubbelklik vervolgens op de computernaam (Figuur 31, helemaal links) om de instellingen voor de dienst aan te passen.



Figuur 32: Web Proxy Service

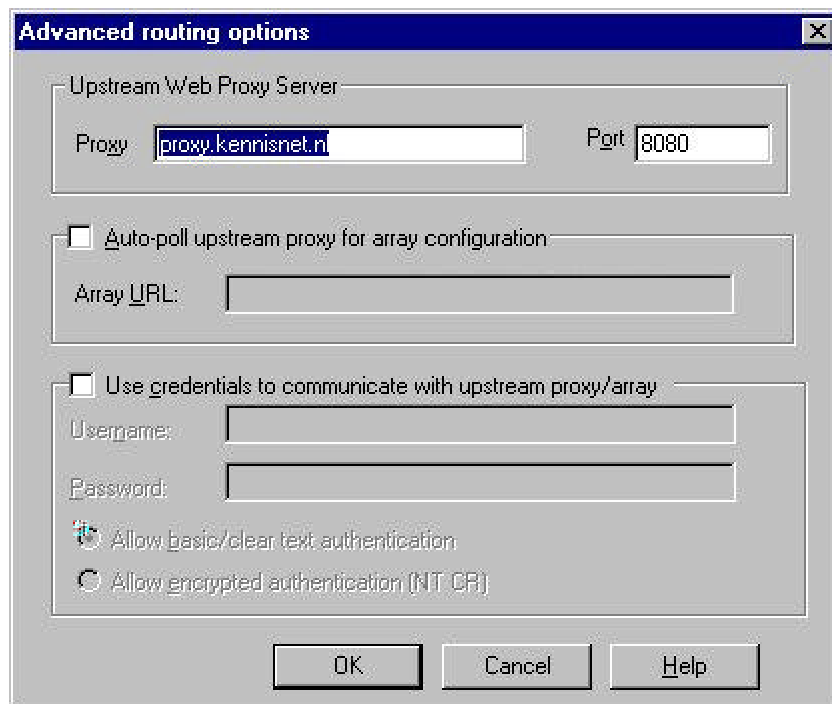


Figuur 33: Web Proxy Routing

Op het tabblad 'Service' (Figuur 32) kunt u enkele zaken instellen, waaronder een omschrijving van de dienst achter 'Comment:'. Deze opties dient u naar eigen inzicht en behoefte in te vullen; raadpleeg hiervoor uw handleiding van de Microsoft Proxy.

Op het tabblad 'Routing' (Figuur 33) dient u in het invulveld de machinenaam in te vullen, ofwel de naam waarnaar verwezen kan worden als zijnde de proxyserver. Het is bij het instellen van de bladerprogramma's van belang om te weten dat u daarvoor de Microsoft Proxy-poort 80 (en niet poort 8080!!!) dient te gebruiken.

In het vakje 'Upstream Routing' dient u de optie 'Use Web Proxy or array' te selecteren. Klik vervolgens op de knop 'Modify...' om de instellingen aan te passen.



Figuur 34: Advanced routing options

Er verschijnt een venster (Figuur 34). Vul achter 'Proxy' in 'proxy.kennisnet.nl' en geef poortnummer '8080' achter 'Port'. Laat de andere opties op het tabblad **uit**geschakeld. Sluit het venster met een klik op 'OK'. Sluit de opties voor de proxyserver om terug te keren naar 'Internet Service Manager'.

3.2.4 Squid

Van Squid zijn twee werkende configuratievoorbeelden beschikbaar: één voor versie 1.2.x en één voor 2.2.x. De relevante gedeelten worden hier weergegeven. In het standaard meegeleverde voorbeeld kunt u deze stukken eenvoudig terugvinden en aan de hier gegeven voorbeelden aanpassen.



Squid kan worden opgehaald van `http://www.squid-cache.org/`.

Scholen kunnen niet zonder meer een proxyserver installeren; het is namelijk belangrijk aan te geven in het configuratiebestand (`squid.conf`), dat deze op zijn beurt weer gebruik moet maken van de proxyservers van kennisnet. Dit is noodzakelijk omdat binnen kennisnet alleen op het Internet gesurft kan worden via een proxyserver.

3.2.4.1 Squid 1.2.x

Parents

Allereerst dienen de zogenaamde 'parent hosts' te worden gedefinieerd. Dit zijn de machines waar uw proxy aan kan refereren om gegevens op te vragen, wanneer deze zich niet in de lokale buffer ('cache') bevinden of wanneer de geldigheid van de betreffende gegevens is verlopen.

```
cache_host proxy.kennisnet.nl parent 8080 3130 no-query
```

Domeingrenzen (versie 1.x.x)

U dient met een aantal zaken de in de buffers op te nemen gegevens in te perken. U kunt dit wellicht het beste op basis van de domeinnaam doen.

De inperking van het te bufferen domein kunt u controleren met de optie 'inside_firewall':

```
inside_firewall kennisnet.nl
```

Met 'local_domain' geeft u het lokale domein aan:

```
local_domain kennisnet.nl
```

3.2.4.2 Squid 2.2.x

Als eerste moet u Squid vertellen wat zijn 'parent cache proxy' is; daarna moet de proxyserver weten dat hij nooit direct verbinding moet gaan zoeken met de betreffende hosts, maar dat deze dat altijd via de proxyserver van kennisnet moet gaan doen.

U kunt dit doen door de volgende regels in uw configuratiefile toe te voegen:

```
cache_peer proxy.kennisnet.nl parent 8080 3130 no-query default
acl all src 0.0.0.0/0.0.0.0
never_direct allow all
```

In principe is dit de enige aanpassing die u in het standaardconfiguratiebestand van Squid hoeft aan te maken om gebruik te kunnen maken van een eigen proxyserver binnen kennisnet. Wel zult u voor optimale prestaties zelf moeten inschatten hoeveel geheugen en diskruimte Squid kan en mag gebruiken.

Domeingrenzen (versie 2.x.x)[4]

In nieuwere versies zijn de opties 'inside_firewall', 'local_domain', 'local_ip' en 'firewall_ip' niet meer beschikbaar. Er wordt in versie 2.0.0 en hoger gebruikgemaakt van de sleutelwoorden 'never_direct' en 'always_direct'. Verder dient in de zogenaamde ACL's (Access Control Lists) te worden aangeven voor welke adressen de 'parents' wel of niet gebruikt mogen worden.

Compleet voorbeeld

Een compleet configuratievoorbeeld voor Squid versie 2.2 stable 5 vindt u in Bijlage B.

3.2.4.3 Overige opties

Verdere opties zult u naar eigen inzicht moeten wijzigen. Deze hebben vooral betrekking op de buffergrootte, de afhandeling van verzoeken, logbestanden en beveiliging. Hiervoor kunt u het beste de documentatie die is bijgevoegd, lezen, of u kunt de documentatie op het Internet raadplegen: http://squid.nlanr.net/Squid/Users-Guide/.

[4] Met dank aan Jeroen Oldenhof, systeembeheerder Drenthecollege.

3.3 Kunnen we zelf filtering toepassen? Hoe?

U kunt zelf, indien uw proxyserver daartoe in staat is dan wel met een programmamodule kan worden uitgebreid, filters instellen om informatie te filteren, waarvan u niet wilt dat uw gebruikers hier toegang toe hebben.

Hoe het precies werkt, is afhankelijk van het product dat u gebruikt. Vaak kunt u een lijst met hetzij verboden, hetzij toegestane adressen opgeven. Bij sommige pakketten kunt u categorieën van adressen selecteren, die bepaalde personen wel of niet mogen opvragen. Bij dergelijke systemen kunt u via de leverancier vaak een abonnement afsluiten om regelmatig nieuwe filterinformatie te ontvangen.

Hoofdstuk 4. Een eigen mailserver

4.1 Kan ik mijn lokale mailserver blijven gebruiken?

Ja, dat kan. U dient hiervoor een verzoek in te dienen bij het Servicepunt kennisnet. U dient een eigen domeinnaam aan te vragen, voorzover u hierover nog niet beschikt. Hierin kan door kennisnet, als Internet Service Provider, worden voorzien. Alle e-mail voor uw eigen domein zal worden doorgestuurd naar uw eigen mailserver. U dient uw lokale mailserver zo in te stellen, dat deze de mailservers van kennisnet (`smtp.kennisnet.nl`) als *smart host* of als *mailrelay* gebruikt voor uitgaande mail.

Er is nog niet voorzien in een mogelijkheid om uw mail weer van buiten kennisnet op te halen vanaf uw lokale mailserver. Technisch gezien is het wel mogelijk, maar dit vereist toestemming van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het zal nader moeten worden bepaald of, en zo ja, hoe in deze mogelijkheid zal worden voorzien.

Om u enigszins op weg te helpen, wordt hier van mailsystemen waarvan deze informatie bekend is, beschreven hoe deze kunnen worden ingesteld voor gebruik op kennisnet.

4.1.1 Sendmail

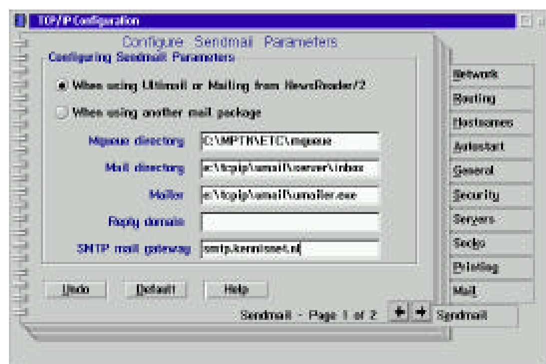
Veruit het meest gebruikte mailsysteem op het Internet is Sendmail. Sendmail is beschikbaar voor vrijwel iedere UNIX-variant en OS/2. Om Sendmail zodanig te configureren dat de mailservers van kennisnet als 'smart host' gebruikt worden, dient u het configuratiebestand aan te passen. Over het algemeen is de configuratie van Sendmail bepaald niet eenvoudig, maar deze handeling is relatief eenvoudig.

Voor UNIX-varianten zijn de instructies als volgt. Open het bestand '`/etc/sendmail.cf`' in uw favoriete editor en zoek naar de letters 'DS' aan het begin van de regel. Eventueel kunt u ook zoeken naar het woord 'relay', daar de optie veelal van een commentaarregel voorafgegaan wordt. Voor OS/2 dient u gebruik te maken van de beheerinterface bij de TCP/IP-configuratie

Direct achter 'DS', dus zonder spatie, vult u de naam van de mailservers van kennisnet in, namelijk '`smtp.kennisnet.nl`'. Hieronder volgt een fragment uit een configuratiebestand.

```
# "Smart" relay host (may be null)
DS
```

Voor OS/2 Sendmail opent u het configuratievenster voor TCP/IP (LAN).



Ga naar het tabblad 'Sendmail'. Dit tabblad bestaat uit twee pagina's, maar alleen de eerste is nu van belang. Vul in het onderste veld, 'SMTP mail gateway', de naam van de mailservers van kennisnet in: `smtp.kennisnet.nl`.

Indien nodig kunt u Sendmail zo instellen, dat het bij een herstart van het systeem automatisch wordt opgestart. Hiervoor dient u op het tabblad 'Autostart' de optie 'Autostart service' voor Sendmail in te schakelen.

Figuur 35: OS/2 Sendmail-configuratie

Meer informatie over Sendmail en de configuratie hiervan kunt u vinden op de website van Sendmail: http://www.sendmail.org/.

4.2 Ik kan niet via POP of IMAP bij mijn eigen webserver vanaf het Internet. Hoe kan ik *toch* de e-mail lezen vanaf het Internet?

Bij sommige mailservers zit de mogelijkheid om een webmailserver aan uw eigen mailserver te koppelen. Soms is deze functie zelfs geïntegreerd in het systeem. Ook bestaan er softwarepakketten om een eigen webmailserver op te zetten en deze via bijvoorbeeld IMAP uw 'normale' mailserver te laten raadplegen.

Kortweg: via een webinterface kunt u uw e-mail beschikbaar maken. Behalve het opzetten van een webmailserver dient u een verzoek in te dienen voor ‘reverse proxy’.

Hoofdstuk 5. Een eigen webserver

5.1 Wat zijn de voordelen van het opzetten van een eigen webserver en van een plek in het webhotel?

U bent uiteraard helemaal vrij in de keuze om een eigen webserver in te richten of gebruik te maken van het webhotel om uw webpagina aan de buitenwereld aan te bieden. Beide opties hebben zo hun voor- en nadelen. Zo heeft een eigen webserver het grote voordeel dat u alle vrijheid hebt om te doen en te laten wat u wilt met de inhoud en scripting, de hoeveelheid schijfruimte etc. Uw eigen website staat bovendien dicht bij uw eigen gebruikers (leerlingen en docenten).

Aan de andere kant dient u dan wel over een machine voor dit doel te beschikken met voldoende capaciteit en zult u – als u uw website wilt publiceren op kennisnet – moeten overwegen meer bandbreedte in te kopen voor uw aansluiting op kennisnet. U moet bovendien de machine zelf beheren, terwijl dat in het geval van het webhotel voor u wordt gedaan.

Indien u uw eigen webserver op het Internet 'zichtbaar' wilt maken, moet u via het Servicepunt kennisnet een verzoek voor een 'reverse proxy' indienen.

5.2 Wat is een 'reverse proxy'?

Om dat uit te leggen, dient u iets te weten over het HTTP-protocol. Het is niet moeilijk, echt! Wat u niet ziet, is wat uw bladerprogramma werkelijk doet wanneer er een bestand of pagina wordt opgevraagd. Het simpelst mogelijke verzoek om bijvoorbeeld de hoofdpagina van een server te krijgen, is het volgende.

```
GET / HTTP/1.0
```

Een korte uitleg. Het verzoek begint met een commando. In dit geval wordt 'GET' gebruikt, maar er zijn meer commando's, doch deze zijn op dit punt niet zo relevant. Na een spatie volgt het gevraagde object (in dit geval de hoofdpagina, aangeduid met '`/`') en na nogmaals een spatie 'HTTP', een schuine streep en het versienummer van het protocol.

Na deze regel zouden nog enkele opties kunnen volgen van de vorm `Optie: waarde`'. In een dergelijke optieregel kan het bladerprogramma zich voorstellen, vertellen welke taal u prefereert, etc. Na alle opties volgt een lege regel, waarna de webserver zal antwoorden.

Op dit moment is versie 1.1 de meest gangbare versie van het HTTP-protocol. In HTTP/1.1 is er één vereiste optie, namelijk '`Host:`'. Na '`Host:`' wordt het adres van de website (bijvoorbeeld `www.kennisnet.nl`) gegeven. Deze optie bepaalt welke gegevens de webserver zal retourneren.

```
GET / HTTP/1.1
Host: www.kennisnet.nl
```

Op basis van deze naam zullen de gegevens uit een bepaalde map worden opgehaald.

De reverse proxy werkt eigenlijk op dezelfde manier, maar niet met lokale mappen. De reverse proxy heeft een tabel met de hostnamen van websites binnen kennisnet, waarvoor een reverse proxy is ingericht. Naast de hostnamen zijn de IP-adressen of echte namen van de webservers vermeld. Wanneer een verzoek binnenkomt voor bijvoorbeeld `www.school.nl`, dan wordt het bijbehorende adres gezocht voor de echte webserver en maakt de reverse proxyserver een verbinding met deze machine. Het binnengekomen verzoek wordt 1 op 1 doorgestuurd en het antwoord wordt weer netjes teruggegeven aan het verzoekende bladerprogramma.

Wanneer u uw eigen webserver op het Internet beschikbaar wilt laten maken, wordt er een extra regeltje aan de tabel toegevoegd.

5.3 Hoe zet ik een eigen webserver op?

De eerste vraag die u zich moet stellen, is wat u precies wilt gaan doen met uw website en welke middelen u nodig denkt te hebben. Op welk computerplatform wilt u uw website opzetten? Als u dat weet, kunt u bepalen welke webserver u gaat gebruiken.

Voor een aantal webservers zal hier worden uitgelegd hoe u deze kunt opzetten.

5.3.1 Apache

Apache is veruit de meest gebruikte webserver. Apache is gratis en voor zeer veel besturingssystemen (vooral UNIX-achtige, maar ook OS/2 en Windows NT) beschikbaar. Via `http://www.apache.org/` kunt u aan de meest recente versie van Apache komen, vaak al voorgecompileerd (lees: kant en klaar) voor uw besturingssysteem.

Bij de meeste Linux-distributies is de installatie van Apache niet veel meer dan het installeren van het juiste pakketje. Daarna kunt u met de hand het proces starten of zal de webservice bij het opstarten van Linux automatisch worden gestart.

Nu begint het echte werk! Het is belangrijk om te weten waar Apache is geïnstalleerd op uw systeem. De standaardlocatie verschilt vrij sterk tussen verschillende distributies en besturingssystemen. De installatie van Apache vindt u bij de volgende systemen in de erbij vermelde mappen.

RedHat Linux en Linux PPC	configuratie	`/etc/httpd/conf`
	logbestanden	`/etc/httpd/logs`
	webpagina's	`/home/httpd/html`
	CGI-programma's	`/home/httpd/cgi-bin`
Slackware Linux	configuratie	`/var/lib/httpd/conf`
	logbestanden	`/var/lib/httpd/logs`
	webpagina's	`/var/lib/httpd/docs`
	CGI-programma's	`/var/lib/httpd/cgi-bin`

Over het algemeen zal uw webserver zonder aanpassingen kunnen functioneren, maar het is niet onverstandig om de configuratiebestanden te controleren en eventueel opties bij te werken. Hoogstwaarschijnlijk treft u de volgende bestanden aan in de configuratiemap.

- **`httpd.conf`** Dit bestand bevat de basisconfiguratiegegevens, zoals het aantal subprocessen dat gestart moet worden, te reserveren capaciteit, etc.
- **`access.conf`** Dit bestand bevat informatie over door wie en vanaf waar bepaalde gegevens mogen worden bekeken.
- **`srm.conf`** In dit bestand worden overige opties, zoals aanvullende bestandsassociaties, koppelingen van typen bestanden aan benamingen en icoontjes gedefinieerd.
- **`mime.types`** Dit bestand bevat een lijst van zogenaamde MIME-types (gestandaardiseerde aanduidingen voor bestandsformaten), gekoppeld aan de bestandsnaam-extensie (`.txt`, `.html`, `.gif` en dergelijke).

De trend is thans om alle configuratieopties weer, zoals dat een paar jaar geleden gebruikelijk was, onder te brengen in alleen '`httpd.conf`'. In alle genoemde bestanden is bij de opties reeds voorzien in beknopte uitleg van de functie. Meer informatie kunt u echter vinden op `http://www.apache.org/`, onder 'Documentation'.

Wanneer de configuratie naar uw zin is, herstart u de webserver (alleen het proces, niet de hele computer!). Dit doet u vaak als root met een commando zoals één van onderstaande.

- `/etc/rc.d/init.d/httpd restart` (RedHat/LinuxPPC)
- `/etc/rc.d/httpd restart` (SuSe)
- `/etc/init.d/httpd restart` (Solaris)
- ``kill -HUP `cat /var/lib/httpd/logs/httpd.pid` `` (Slackware)

U kunt nu uw webpagina's plaatsen in de juiste map. Zorg wel dat het webserverproces de bestanden kan lezen (type `man chmod`' voor meer informatie op een UNIX-systeem). Door nu met een bladerprogramma uw website te benaderen, kunt u bekijken of het eruit ziet, zoals u dat in gedachten had.

5.3.2 MacOS Persoonlijke webserver

Bij de meer recente versies van MacOS zit standaard een 'Persoonlijke webserver'. Hiermee kunt u zeer eenvoudig een eigen webserver opzetten. U hoeft de webserver eigenlijk alleen maar in te schakelen. Zorg wel dat uw TCP/IP-instellingen correct zijn!



Figuur 36: regelpaneel 'Extensiebeheer'

Op de regelbalk, welke zich normaliter onder aan uw beeld bevindt, staat een klein icoontje, waar een menu bij hoort. Via dit menu kunt u de webserver aan- en uitschakelen ('Schakel webserver in').

Controleer allereerst of op uw systeem de 'webserver-extensie' is ingeschakeld. Open het regelpaneel 'Extensiebeheer' (Control Panel: 'Extensions').

Zoek in de lijst de 'Webserver-extensie' op. Als er een kruisje voor deze extensie staat, dan is deze reeds actief. Indien dat niet het geval is, klik dan op het vierkantje om de extensie in te schakelen en klik vervolgens op 'Herstart'.

Na een eventuele herstart kunt u de webserver activeren via de regelbalk.



Figuur 37: regelbalk: Persoonlijke webserver



Figuur 38: regelpaneel Webserver

Wanneer u nog zaken wilt instellen, dan kunt u dat via het regelpaneel 'Webserver' doen. Open, via de regelbalk of via het Apple-menu, deze regelbalk om het venster zoals weergegeven in Figuur 38 te openen.

Standaard is de locatie waar uw webpagina's zich bevinden '`<disknaam>:Webpagina's`' (voor anderstalige versies van MacOS zal dit afwijken). Dit kunt u met de bovenste 'Selecteer...'-knop aanpassen. De onderste 'Selecteer...'-knop kunt u benutten om een specifieke naam te gebruiken voor de openingspagina van een map. Selecteer bijvoorbeeld 'Standaard.html'.

U kunt in dit regelpaneel ook de webserver stoppen en starten. Bovendien bestaat hier de mogelijkheid om mensen toegang te geven tot de bestanden op basis van Samengebruik-profielen. Het wordt **niet** aangeraden om dit in te schakelen, tenzij u **echt** weet wat u doet!

Als alles is ingeschakeld en geconfigureerd, kunt u de website benaderen via het adres van uw Mac-server. Wanneer u uw webserver hebt gestart, zijn de mogelijke adressen ook te zien in het regelpageel 'Webserver' bij 'Mijn adres'.



Figuur 39: de standaardopeningspagina

De 'MacOS Persoonlijke webserver' biedt geen bijzondere mogelijkheden, maar is een snelle en eenvoudige oplossing voor een eigen webserver.

5.4 Wat is CGI? En hoe werkt dat?

CGI is de afkorting voor 'Common Gateway Interface'. CGI zorgt ervoor dat er op basis van gebruikersinvoer dynamisch webpagina's gegenereerd kunnen worden. Als u bijvoorbeeld een formulier op een webpagina invult en dan op de verzendknop klikt, wordt er informatie van uw bladerprogramma naar de webserver verstuurd. Dit kan grofweg op twee manier. Het HTTP-protocol kent hiervoor het GET-commando en het POST-commando.

In het geval van het GET-commando wordt er een verlengd adres gegenereerd. Uw bladerprogramma krijgt bijvoorbeeld de instructie om bij het klikken op de verzendknop het adres `http://www.school.nl/cgi-bin/formulier.pl` op te roepen. Achter dit adres wordt vervolgens een vraagteken geplaatst en een lijst van parameters met waarden, gescheiden door een ampersand (&): `?parameter1=waarde&parameter2=waarde2`

Dit resulteert dan in een volledig adres als:

`http://www.school.nl/cgi-bin/formulier.pl?a=jan&b=jansen`

De parameters en waarden worden overigens wel op een dusdanig manier gecodeerd, dat speciale tekens in de parameternamen en in de waarden netjes worden geïnterpreteerd. Speciale tekens zijn onder andere het ampersandteken (&), spaties, plusteken (+), is-teken (=) etc.

Het deel achter het vraagteken wordt door middel van een variabele aan een programma op de server doorgegeven. Dit programma kan de gegevens decoderen en opsplitsen. Op basis van de gegevens zal het bepaalde acties uitvoeren en een nieuwe webpagina, een afbeelding, tekst of iets dergelijks genereren.

Het verschil met het POST-commando is tweeledig. Enerzijds is de overdracht van informatie van het bladerprogramma naar de webserver anders, anderzijds is de manier waarop het betreffende programma op de webserver de informatie aangeleverd krijgt, anders.

Het adres dat het bladerprogramma krijgt, wordt ongemoeid gelaten. In plaats daarvan wordt de informatie niet in het verzoek, maar direct na het verzoek en alle HTTP-protocolparameters meegezonden naar de webserver.

Het CGI-programma krijgt de informatie via 'standaard invoer'. Dat wil zeggen dat het voor het CGI-programma lijkt alsof de invoer van het toetsenbord komt (wat uiteraard niet het geval is). Het CGI-programma leest de informatie teken voor teken in en verwerkt deze. Op basis van de gegevens zal het verder op dezelfde manier kunnen handelen als bij een GET-verzoek. Het is ook mogelijk om CGI-programma's te maken die met beide soorten verzoeken om kunnen gaan. Vaak wordt die mogelijkheid gebruikt om in het geval van een GET-verzoek (de standaard van een bladerprogramma) een formulier te genereren. De informatie wordt daarna via POST verstuurd.

Belangrijk is dat uw webserver moet weten dat een bepaald bestand een CGI-programma is en als zodanig uitgevoerd moet worden wanneer het aangeroepen wordt. Het kan bepaald worden door de map waarin het programma geïnstalleerd is, maar soms ook door de extensie van de bestandsnaam. Hoe dit exact moet worden aangegeven, hangt af van de configuratie van uw webserver; raadpleeg eventueel de documentatie.

5.5 Hoe maak ik een CGI-programma?

Allereerst mag u kiezen welke programmeertaal u wilt gebruiken. CGI kan in elke willekeurige programmeertaal worden geschreven, die op uw platform beschikbaar is. Een zeer veel gebruikte programmeertaal (scripttaal) is Perl. Perl is voor zeer veel besturingssystemen beschikbaar. Daarvan wordt hier een voorbeeld gegeven.

Het eerste dat een CGI-programma moet doen, is aan de webserver vertellen welk soort informatie zal volgen. Hiervoor dient het een regel beginnend met 'Content-Type:' te printen. Achter 'Content-Type:' volgt het soort informatie:

- webpagina: `text/html`
- platte tekst: `text/plain`
- GIF-afbeelding: `image/gif`
- JPEG-afbeelding: `image/jpeg`
- Word-document: `application/msword`
- etc.

Hierna volgen eventueel andere opties, een lege regel en daarna de inhoud.

Een heel eenvoudig CGI-script is het volgende[5], geschreven in Perl:

```
#!/usr/local/bin/perl
$|=1;
printf "Content-Type: text/html\n";
printf "\n";
printf "<html><body><h1>Hello, World!</h1></body></html>\n";
```

Een simpele paginateller, die een klein icoontje teruggeeft als onderdeel van een webpagina, zou er als volgt uit kunnen zien:

[5] Sommige mensen beweren dat het ongeluk brengt om te leren programmeren en 'Hello, World!' over te slaan.

```
#!/usr/local/bin/perl
$|=1;
printf "Content-Type: image/gif\n";
printf "\n";
system("cat /home/httpd/icons/count.gif");
my $COUNT=`cat /home/httpd/etc/pagecount.txt`; chop $COUNT;
$COUNT++;
open(STATS, "/home/httpd/etc/pagecount.txt");
printf STATS "%d\n", $COUNT;
close STATS;
```

Dit script leest een bestand met de huidige stand en schrijft de nieuw stand weer weg in dat bestand. Ondertussen stuurt het de inhoud van een GIF-bestandje terug naar het bladerprogramma.

Een derde voorbeeld laat zien hoe de invoer via een POST-verzoek kan worden verwerkt, en zou bij uitvoering een lijstje laten zien van de invoerparameters:

```
#!/usr/local/bin/perl
$|=1;

# Forward declarations

sub http_header;
sub html_start;
sub html_finish;

http_header();

if ($ENV{'REQUEST_METHOD'} ne 'POST') {
  html_start('Fout');
  print <<EOM
<h1>Fout</h1>
<p>U heeft dit script waarschijnlijk niet met het juist formulier
aangeroepen</p>
EOM
}
else
{
#-------------------------------------------------------------------------
# Verwerk de invoer
#-------------------------------------------------------------------------
  read(STDIN, $buffer, $ENV{'CONTENT_LENGTH'});

  @pairs = split(/&/, $buffer);

  html_start('Invoer');
  print "<ul>\n";
  foreach $pair (@pairs) {
     ($name, $value) = split(/=/, $pair);

     # Decodeer de parameters
     $value =~ tr/+/ /;
     $value =~ s/%([a-fA-F0-9][a-fA-F0-9])/pack("C", hex($1))/eg;
     $value =~ s/<!--(.|\n)*-->//g;

     if ($allow_html != 1) {
        $value =~ s/<([^>]|\n)*>//g;
     }

     printf "<li><b>%s:</b> %s</li>\n", $name, $value;
  }
  print "</ul>\n";
};
```

```
html_finish();

exit(0);

##########################################################################

sub http_header {
  print "Content-Type: text/html\n\n";
}

sub html_start {
  my($title) = @_;
  print <<EOM;
<html>
<head>
<title>$title</title>
</head>

<body bgcolor="#FFFFFF">

EOM
}

sub html_finish {
  print <<EOM;
</body>
</html>
EOM
}
```

De pad- en bestandsnamen in de scripts zullen verschillen bij gebruik op uw eigen machine, zeker wanneer het een Windows- of Macintosh-systeem betreft.

Meer informatie over HTML-formulieren, JavaScript en CGI kunt u vinden op http://developer.netscape.com/.

Hoofdstuk 6. IP-adressering en Network Address Translation

6.1 Ik heb al een netwerk binnen de school, waarbinnen ik IP-nummers heb toegekend. Moet ik nu andere nummers gaan gebruiken?

Ja, dat moet. De reeks IP-nummers die men krijgt, is afhankelijk van de IP-leverancier. Ook kennisnet is zo´n IP-leverancier en heeft een eigen nummerreeks.

Dit hoeft geen groot probleem op te leveren. Alle werkstations kunnen in principe met DHCP worden geconfigureerd (zie deel III, Software, voor instructies), zodat de IP-nummers daarvoor automatisch via kennisnet worden verkregen. Alleen eigen servers, LAN-servers bijvoorbeeld, of interne routers *moeten* voorzien worden van vaste (statische) IP-nummers. Zie bijlage A. voor informatie over de statisch toe te kennen IP-nummers.

6.2 Kan ik mijn eigen IP-adressen behouden?

In principe niet. U krijgt een reeks adressen toegewezen, die u dient te gebruiken. Er bestaat echter een truc, NAT (Network Address Translation) of 'masquerading' genoemd, waarmee het mogelijk is om uw interne IP-nummers naar de IP-nummers van kennisnet te vertalen, en weer terug. Er zit ook een schaduwzijde aan NAT of masquerading: niet alle diensten kunnen op deze manier worden gebruikt, doch de belangrijkste diensten wel.

Indien u van NAT of masquerading gebruik wilt maken, is dit geheel uw eigen verantwoordelijkheid en dient u zelf voor de extra apparatuur en programmatuur én het onderhoud daarvan te zorgen. U plaatst dan een eigen 'router' of 'forwarding host' (computer) tussen de kennisnetaansluiting en uw lokale netwerk.

Een andere oplossing zou kunnen zijn om alle applicaties die u wilt gebruiken, via een proxy te laten lopen. Hiertoe dient u zelf een proxyserver op te zetten welke geen routering van IP ondersteunt, of waarop routering (soms ook 'forwarding' genoemd) in ieder geval is uitgeschakeld. Voor websurfen maakt u gebruik van een HTTP-proxy. Voor veel andere protocollen zoals Telnet, Secure Shell (SSH), het ophalen en verzenden van e-mail en IRC kan, indien uw software dit ondersteunt, gebruik worden gemaakt van SOCKS. Er zijn diverse proxypakketten op de markt verkrijgbaar. Via Tucows kunt u, in elk geval voor Windows NT, een aantal commerciële demoversies van dergelijke pakketten ophalen.

Let wel dat uw netwerken in dit geval 'logisch' gescheiden zijn en veel speciale protocollen niet worden ondersteund door proxyservers.

6.3 Hoe werkt 'Network Address Translation' (NAT)?

Network Address Translation, kortweg NAT, zorgt ervoor dat adressen aan de ene kant van een router vertaald worden naar adressen aan de andere kant van de router, zodat er verkeer mogelijk wordt gemaakt door de router. Dit kan nuttig zijn wanneer u op een lokaal netwerk adressen gebruikt, die normaliter niet bruikbaar zijn buiten het lokale netwerk.

Er zijn verschillende vormen van NAT: 1 op 1-vertaling, 1 op *n*-vertaling en *n* op *m*-vertaling. Meer informatie kunt u vinden in een afstudeerscriptie van een Duitse student:

http://www.csn.tu-chemnitz.de/~mha/linux-ip-nat/diplom/.

In dit Engelstalige document wordt duidelijk en zeer gedetailleerd uitgelegd hoe de verschillende vormen van NAT werken.

De meest voorkomende variant van NAT is 'masquerading', waarbij alle adressen van het interne netwerk worden vertaald naar slechts één IP-adres aan de buitenkant van het netwerk.

6.4 Wat zijn de beperkingen van NAT/masquerading?

Het gebruik van NAT wordt over het algemeen door de experts niet aangeraden. NAT is een truc en geen oplossing voor de lange termijn. NAT is onder andere ooit bedoeld om problemen met de schaarste van IP-adressen op te vangen en om het eenvoudiger te maken om een aansluiting te verhuizen (zonder het interne netwerk te hoeven omnummeren). De reden dat NAT of masquerading desondanks wordt afgeraden, heeft ermee te maken dat niet alle protocollen bestand zijn tegen adresvertaling. Soms is dit op te lossen, maar niet altijd.

Een bekend voorbeeld is FTP. Overigens is het probleem in dit geval in nagenoeg alle NAT-implementaties opgelost. Ter illustratie wordt hier uitgelegd wat er gebeurt tijdens het FTP'en.

FTP maakt gebruik van twee verbindingen. Allereerst wordt een verbinding opgezet om de overdracht van bestanden en informatie te bedienen ('Control Channel'). Telkens wanneer er een bestand of informatie opgevraagd of verzonden moet worden, wordt er een tweede verbinding opgezet ('Data Channel'). Het IP-adres en het TCP-poortnummer van het 'Control Channel' worden bepaald door de server en zijn een vast gegeven, maar het IP-adres en het TCP-poortnummer van het 'Data Channel' worden dynamisch bepaald door de clientapplicatie.

Om het 'Data Channel' te openen, stuurt de applicatie het volgende commando (de getoonde getallen zijn slechts voorbeelden):

```
PORT 10,1,1,153,8,24
```

Dit commando heeft zes parameters, gescheiden door komma's. De eerste vier parameters vormen samen de vier delen van het IP-adres: **10**.**1**.**1**.**153**. De laatste twee parameters vormen samen het betreffende TCP-poortnummer: **8***256 + **24** = 2072.

De FTP-server zal op dat moment dus een verbinding proberen te maken met het IP-adres 10.1.1.153 op TCP-poort 2072. Indien dat slaagt, volgt het volgende antwoord:

```
200 PORT command successful.
```

Indien er een NAT-systeem tussen zou zitten, zou de applicatie een intern en onbereikbaar adres doorgeven in het PORT-commando. Het adres van de NAT-gateway (aan de buitenkant) is bijvoorbeeld 212.178.1.1 en dat is het enige adres dat de FTP-server kan bereiken. Wanneer de FTP-server een verbinding zou proberen op te zetten met 10.1.1.153, zou dat niet lukken.

Om te voorkomen dat de FTP-server met 10.1.1.153 zou verbinden, moet de NAT-gateway actief het FTP-verkeer op het 'Control Channel' in de gaten houden. Wanneer er een PORT-commando voorbijkomt, dient dit te worden afgevangen. De NAT-gateway vervangt de eerste vier parameters, zodat het IP-adres 212.178.1.1 wordt vermeld. De NAT-gateway bepaalt zelf een willekeurig poortnummer en vult dat in voor de laatste twee parameters. Het resultaat wordt dan bijvoorbeeld:

```
PORT 212,178,1,1,235,74
```

Wanneer de FTP-server dan een 'Data Channel' opzet naar 212.178.1.1, TCP-poort (235*256+74=) 60234, maakt de NAT-gateway een verbinding met 10.1.1.153, TCP-poort 2072 en stuurt het verkeer tussen de beide verbindingen door.

Om te zorgen dat de NAT-gateway deze truc kan uitvoeren, zijn extra controles nodig op het verkeer. Dit maakt de NAT-gateway een stuk complexer. Een dergelijke truc kan helaas niet voor alle protocollen worden uitgehaald, zeker niet wanneer het verkeer wordt gecodeerd. Soms biedt een (SOCKS-)proxyserver in dat geval uitkomst.

6.5 Kan ik meer IP-nummers krijgen? Ik heb er te weinig gekregen van kennisnet.

Dat kan indien u de noodzaak ervan kunt aantonen. Hiertoe dient u een **beargumenteerd** en **gespecificeerd** verzoek in te dienen bij het Servicepunt kennisnet. Houdt u er rekening mee dat u bepaalde instellingen in uw netwerk zult moeten aanpassen, omdat niet gegarandeerd kan worden dat de nieuwe nummers aansluiten op de thans aan u toegewezen reeks.

RIPE-NCC, de autoriteit die voor Europa verantwoordelijk is voor de uitgifte van (publieke) IP-adressen, heeft vrij strikte regels opgesteld voor het gebruik van IP-adressen. Dit vereist dat aangetoond wordt dat extra IP-adressen daadwerkelijk noodzakelijk zijn.

Hoofdstuk 7. Netwerkkoppelingen

7.1 Kan ik mijn Internet-webserver koppelen via kennisnet?

Ja, via een 'reverse proxy' kan vanaf kennisnet toegang worden verkregen tot uw webserver op school. U dient een verzoek in te dienen bij het Servicepunt kennisnet om dit voor u te realiseren. U dient hiervoor, eveneens via het Servicepunt kennisnet, een eigen domeinnaam aan te vragen indien u hierover nog niet beschikt.

7.2 Mogen de leerlingen via de modempool van school het kennisnet op?

Nee, dat is in principe *niet* de bedoeling. Het netwerk van kennisnet is opgezet als een gesloten netwerk en dat zal ook zo blijven. Door een modempool aan het schoolnetwerk te koppelen, creëert u een 'achterdeur' naar het kennisnet. Alleen indien u kunt **garanderen** dat er middels een aanmelding met minimaal een gebruikersnaam en wachtwoord tot uw netwerk toegang kan worden verkregen *én* kunt **garanderen** dat er geen andere gebruikers dan de bestaande gebruikers van kennisnet via uw inbelvoorziening het kennisnet op kunnen, is het toegestaan om een dergelijke voorziening aan uw leerlingen aan te bieden.

7.3 Ik heb al een eigen Internetaansluiting, en nu kennisnet erbij. Wat nu?

U hebt een probleem dat u moet oplossen. Als u al druk gebruikmaakt van uw bestaande aansluiting, is het raadzaam de nieuwe kennisnetaansluiting eerst met een aantal werkstations uit te proberen en dan rustig een migratie te plannen naar een situatie met alleen nog een kennisnetaansluiting. Overleg met het Servicepunt kennisnet is daarbij onontbeerlijk.

In de situatie dat u beide aansluitingen naast elkaar gebruikt, dient u ervoor te zorgen dat er geen vermenging optreedt. Dat betekent dat een lokaal systeem *of* met kennisnet moet praten, *of* met de andere aansluiting – verwarring moet niet mogelijk zijn. **Er mag op geen enkele manier contact onstaan tussen uw Internetaansluiting en uw aansluiting op kennisnet!**

Pas daarbij op: er mag slechts één DHCP-service tegelijk actief zijn, dus als uw bestaande aansluiting ook DHCP biedt (automatische IP-nummertoekenning), dan *moet* dat in de kennisnetaansluiting worden uitgezet (zie paragraaf 1.1).

Als u meteen wilt overstappen, is het raadzaam om de bestaande aansluiting uit te schakelen, zodat eventuele conflicten vermeden worden.

Bij het gebruik van twee aansluitingen tegelijk bent u geheel verantwoordelijk voor mogelijke beveiligingsrisico´s die u voor kennisnet introduceert ('achterdeurtjes').

Nogmaals: in situaties als deze is overleg met het Servicepunt kennisnet onontbeerlijk!

7.4 Er zijn enkele (eigen) routers in het lokale netwerk, die verschillende delen onderling verbinden. Heeft dit consequenties?

Ja, dit heeft wel degelijk consequenties. De computers die zich 'achter' deze router(s) bevinden, dienen de betreffende router als 'default gateway' te gebruiken, in plaats van de gateway die via de centrale DHCP-server van kennisnet wordt doorgegeven. Dit kunt u 'hard' instellen in uw clients, maar beter is waarschijnlijk om een eigen DHCP-server op te zetten, die de juiste gegevens uitdeelt. Zie hiervoor paragraaf 1.1.

Eigenlijk is het gebruik van routers in uw eigen netwerk niet nodig, althans in het geval van een lokaal netwerk, dat behalve de kennisnetaansluiting geen verbindingen heeft met bijvoorbeeld andere locaties van de school. Elke vestiging hoort een eigen kennisnetaansluiting te hebben. Veel beter is om op de locaties zelf een aantal grotere hubs of switches te gebruiken om verschillende segmenten te koppelen. Deze zijn over het algemeen een stuk goedkoper dan routers en vergen beduidend minder, of zelfs geen onderhoud.

U mag in geen geval (met behulp van routers) een verbindingen maken met IP-netwerken die niet tot kennisnet behoren.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen aan 'handboek@kennisnet.nl'.

Bijlage B. Voorbeeldconfiguratie Squid 2.2 stable 5

Deze bijlage geeft een configuratie die in de praktijk heeft bewezen te werken met Squid versie 2.2 stable 5. Hierbij wordt gebruikgemaakt van de proxyservers van kennisnet. Iedereen is vrij dit bestand te gebruiken, maar wel geheel op eigen risico. De belangrijkste punten voor deze configuratie:

- zal altijd al haar verzoeken forwarden naar de proxyserver van kennsinet;
- luistert op poort 8080;
- heeft een geheugenbuffer van 8 MB (mag groter zijn!);
- deze Squid-configuratie zal al haar benodigde files zoeken in `/usr/local/squid/` (LET OP! De exacte locatie verschilt nogal eens tussen verschillende UNIX-varianten en -distributies);
- Squid zal geen DNS-informatie opzoeken;
- geschikt om gebruik te maken van de cache manager (`cachemgr.cgi`).

Verder wordt het aangeraden om het systeem zo te optimaliseren, dat het geheugen effectief wordt gebruikt: gebruik wat u kunt missen. Ongeveer de helft tot driekwart van het fysiek aanwezige geheugen is waarschijnlijk een goede keuze. Zet bij voorkeur een machine speciaal als proxy in om de prestaties zo hoog mogelijk te houden.

```
# Generated automatically from squid.conf.pre.in by configure.
#
# $Id: squid.conf.pre.in,v 1.93.2.16 1998/05/01 23:21:03 wessels Exp $
#

#  TAG: http_port
#       The port number where squid will listen for HTTP client
#       requests.  Default is 3128, for httpd-accel mode use port 80.
#       May be overridden with -a on the command line.
#
http_port 8080

#  TAG: icp_port
#       The port number where squid send and receive ICP requests to
#       and from neighbor caches.  Default is 3130.  To disable use
#       "0".  May be overridden with -u on the command line.
#
icp_port 0

#  TAG: mcast_groups
#       This tag specifies a list of multicast groups which your
#       server should join to receive multicasted ICP requests.
#
#       NOTE!  Be very careful what you put here!  Be sure you
#       understand the difference between an ICP _query_ and an ICP
#       _reply_.  This option is to be set only if you want to RECEIVE
#       multicast queries.  Do NOT set this option to SEND multicast
#       ICP (use cache_host for that).  ICP replies are always sent via
#       unicast, so this option does not affect whether or not you will
#       receive replies from multicast group members.
#
#       You must be very careful to NOT use a multicast address which
#       is already in use by another group of caches.  NLANR has been
#       assigned a block of multicast address space for use in Web
```

```
#       Caching.  Plese write to us at nlanr-cache@nlanr.net to receive
#       an address for your own use.
#
#       Usage:  mcast_groups 239.128.16.128 224.0.1.20
#
#       By default, squid doesn't listen on any multicast groups.
#
#mcast_groups 239.128.16.128

#  TAG: tcp_incoming_address
#  TAG: tcp_outgoing_address
#  TAG: udp_incoming_address
#  TAG: udp_outgoing_address
#
#       Usage: tcp_incoming_address 10.20.30.40
#              udp_outgoing_address fully.qualified.domain.name
#
#       These tags have replaced 'bind_address' and 'outbound_address'
#       to provide more control for multihomed hosts.
#
#       tcp_incoming_address    is used for the HTTP socket which accepts
#                               connections from clients and other caches.
#       tcp_outgoing_address    is used for connections made to remote
#                               servers and other caches.
#       udp_incoming_address    is used for the ICP socket receiving packets
#                               from other caches.
#       udp_outgoing_address    is used for ICP packets sent out to other
#                               caches.
#
#       The defaults behaviour is to not bind to any specific address.
#
#       NOTE, udp_incoming_address and udp_outgoing_address can not have
#       the same value since they both use port 3130.
#
#tcp_incoming_address 0.0.0.0
#tcp_outgoing_address 0.0.0.0
#udp_incoming_address 0.0.0.0
#udp_outgoing_address 0.0.0.0

# OPTIONS WHICH AFFECT THE NEIGHBOR SELECTION ALGORITHM
#-----------------------------------------------------------------------------
--

#  TAG: cache_host
#       To specify other caches in a hierarchy, use the format:
#
#           hostname type http_port icp_port
#
#   For example,
#
#       #                                         proxy  icp
#       #          hostname             type     port   port  options
#       #          -------------------- -------- ----- ----- -----------
#       cache_host bigserver.usc.edu    parent    3128  3130  [proxy-only]
#       cache_host littleguy1.usc.edu   sibling   3128  3130  [proxy-only]
#       cache_host littleguy1.usc.edu   sibling   3128  3130  [proxy-only]
#
#             type:  either 'parent', 'sibling', or 'multicast'.
```

```
#
#       proxy_port:  The port number where the cache listens for proxy
#                    requests.
#
#         icp_port:  Used for querying neighbor caches about
#                    objects.  To have a non-ICP neighbor
#                    specify '7' for the ICP port and make sure the
#                    neighbor machine has the UDP echo port
#                    enabled in its /etc/inetd.conf file.
#
#           options: proxy-only
#                    weight=n
#                    ttl=n
#                    no-query
#                    default
#                    round-robin
#                    multicast-responder
#
#                    use 'proxy-only' to specify that objects fetched
#                    from this cache should not be saved locally.
#
#                    use 'weight=n' to specify a weighted parent.
#                    The weight must be an integer.  The default weight
#                    is 1, larger weights are favored more.
#
#                    use 'ttl=n' to specify a IP multicast TTL to use
#                    when sending an ICP request to this address.
#                    Only useful when sending to a multicast group.
#                    Because we don't accept ICP replies from random
#                    hosts, you must configure other group members as
#                    peers with the 'multicast-responder' option below.
#
#                    use 'no-query' to NOT send ICP queries to this
#                    neighbor.
#
#                    use 'default' if this is a parent cache which can
#                    be used as a "last-resort." You should probably
#                    only use 'default' in situations where you cannot
#                    use ICP with your parent cache(s).
#
#                    use 'round-robin' to define a set of parents which
#                    should be used in a round-robin fashion in the
#                    absence of any ICP queries.
#
#                    'multicast-responder' indicates that the named peer
#                    is a member of a multicast group.  ICP queries will
#                    not be sent directly to the peer, but ICP replies
#                    will be accepted from it.
#
#       NOTE: non-ICP neighbors must be specified as 'parent'.
#
#cache_host hostname type 3128 3130

#  TAG: cache_host_domain
#       Use to limit the domains for which a neighbor cache will be queried.
```

```
#       Usage:
#
#       cache_host_domain cache-host domain [domain ...]
#       cache_host_domain cache-host !domain
#
#       For example, specifying
#
#               cache_host_domain bigserver.usc.edu     .edu
#
#       has the effect such that UDP query packets are sent to
#       'bigserver' only when the requested object exists on a
#       server in the .edu domain.  Prefixing the domainname
#       with '!' means that the cache will be queried for objects
#       NOT in that domain.
#
#       NOTE:   * Any number of domains may be given for a cache-host,
#                 either on the same or separate lines.
#               * When multiple domains are given for a particular
#                 cache-host, the first matched domain is applied.
#               * Cache hosts with no domain restrictions are queried
#                 for all requests.
#               * There are no defaults.
#               * There is also a 'cache_host_acl' tag in the ACL
#                 section.

#  TAG: neighbor_type_domain
#
#       usage: neighbor_type_domain parent|sibling domain domain ...
#
#       Modifying the neighbor type for specific domains is now
#       possible.  You can treat some domains differently than the the
#       default neighbor type specified on the 'cache_host' line.
#       Normally it should only be necessary to list domains which
#       should be treated differently because the default neighbor type
#       applies for hostnames which do not match domains listed here.
#
#EXAMPLE:
#       cache_host  parent cache.foo.org 3128 3130
#       neighbor_type_domain cache.foo.org sibling .com .net
#       neighbor_type_domain cache.foo.org sibling .au .de

#  TAG: inside_firewall
#       This tag specifies a list of domains inside your Internet
#       firewall.
#
#       Usage: inside_firewall my.domain  [ my.other.domain ...]
#              !out.my.domain my.domain
#
#       The use of this tag affects the server selection algorithm in
#       two ways.  Objects which do not match any of the listed domains
#       will be considered "beyond the firewall."  For these:
#               - There will be no DNS lookups for the URL-host.
#               - The object will always be fetched from one of
#                 the parent or neighbor caches.
#
```

```
#       As a special case you may specify the domain as 'none' to force
#       all requests to be fetched from neighbors and parents.
#       Prefixing a domain name with '!' means the domain is NOT inside
#       your firewall.
#
#inside_firewall topsecret.com
#inside_firewall kennisnet.nl
cache_peer proxy.kennisnet.nl parent 8080 3130 no-query default
acl all src 0.0.0.0/0.0.0.0
never_direct allow all

#  TAG: local_domain
#       This tag specifies a list of domains local to your organization.
#
#       Usage: local_domain my.domain [ my.other.domain ...]
#
#       For URLs which are in one of the local domains, the object
#       is always fetched directly from the source and never from a
#       neighbor or parent.
#
#local_domain ce.nihon-u.ac.jp

#  TAG: local_ip
#       This tag specifies a list of network addresses local to your
#       organization.
#
#       Usage: local_ip ip-address
#
#       This tag is similar to local_domain, except that the IP-address
#       of the URL-host is checked.  This requires that a DNS lookup
#       be done on the URL-host.  For this reason, local_domain is
#       preferred over local_ip.  By using local_domain it may be
#       possible to avoid the DNS lookup altogether and deliver the
#       object with less delay.
#
#local_ip 10.0.0.0
#local_ip 192.168.0.1

#  TAG: firewall_ip
#
#       Just like 'inside_firewall' but for IP addresses.  NOTE:
#       firewall_ip and local_ip are mutually exclusive.  If you
#       use firewall_ip then local_ip will be ignored.
#
#firewall_ip 10.0.0.0
#firewall_ip 172.16.0.0
#  TAG: single_parent_bypass
#       This tag specifies that it is okay to bypass the hierarchy
#       "Pinging" when there is only a single parent for a given URL.
#
#       Usage: single_parent_bypass on|off
#
#       Before actually sending ICP "ping" packets to parents and
#       neighbors, we figure out which hosts would be pinged based
#       on the cache_host_domain rules, etc.  Often it may be the
```

```
#       case that only a single parent cache would be pinged.
#
#       Since there is only a single parent, there is a very good
#       chance that we will end up fetching the object from that
#       parent.  For this reason, it may be beneficial to avoid
#       the ping and just fetch the object anyway.
#
#       However, if we avoid the ping, we will be assuming that the
#       parent host is reachable and that the cache process is running.
#       By using the ping, we can be reasonably sure that the parent
#       host will be able to handle our request.  If the ping fails then
#       it may be possible to fetch the object directly from the source.
#
#       To favor the resiliency provided by the ping algorithm,
#       single_parent_bypass is 'off' by default.
#
#single_parent_bypass off

#  TAG: source_ping
#       If source_ping is enabled, then squid will include the source
#       provider site in its selection algorithm.  This is accomplished
#       by sending ICP "HIT" packets to the UDP echo port of the source
#       host.  Note that using source_ping may send a fair amount of UDP
#       traffic out on the Internet and may irritate paranoid network
#       administrators.
#
#       Note that source_ping is incompatible with inside_firewall.
#       For hosts beyond the firewall, source_ping packets will never
#       be sent.
#
#       By default, source_ping is off.
#
#source_ping off

#  TAG: neighbor_timeout (seconds)
#       This controls how long to wait for replies from neighbor caches.
#       If none of the parent or neighbor caches reply before this many
#       seconds (due to dropped packets or slow links), then the object
#       request will be satisfied from the default source.  The default
#       timeout is two seconds.
#
#neighbor_timeout 2

#  TAG: hierarchy_stoplist
#       A list of words which, if found in a URL, cause the object to
#       be handled directly by this cache.  In other words, use this
#       to not query neighbor caches for certain objects.  You may
#       list this option multiple times.
#
#       The default is to directly fetch URLs containing 'cgi-bin' or '?'.
#
hierarchy_stoplist cgi-bin ?

#  TAG: cache_stoplist
#       A list of words which, if found in a URL, cause the object to
```

```
#       immediately removed from the cache.  In other words, use this
#       to force certain objects to never be cached.  You may list this
#       option multiple times.
#
#       The default is to not cache URLs containing 'cgi-bin' or '?'.
#
#cache_stoplist cgi-bin ?

#  TAG: cache_stoplist_pattern          # case sensitive
#  TAG: cache_stoplist_pattern/i        # case insensitive
#
#       Just like 'cache_stoplist' but you can use regular expressions
#       instead of simple string matching.  There is no default.
#
#cache_stoplist_pattern

#  TAG: no_cache
#
#       Use ACL elements to specify uncachable objects.  For example,
#       this prevents caching of objects downloaded from servers whose
#       IP addresses are in the 192.172.226.0 network:
#
#       acl FOO dst 192.172.226.0/24
#       no_cache deny FOO
#
#       You MUST use the 'deny' keyword before the list of ACL names.
#       For more details on how to specify ACLs and access lists,
#       See the comments for 'http_access' below, and please read the
#       Squid FAQ (http://squid.nlanr.net/Squid/FAQ/FAQ.html).
#

# OPTIONS WHICH AFFECT THE CACHE SIZE
#-----------------------------------------------------------------------------
--

#
#  TAG: cache_mem (megabytes)
#       Maximum amout of VM used to store objects in memory.
#       This includes:
#               in-transit objects,
#               negative-cached objects,
#               "hot" objects
#       The value of cache_mem is an upper limit on the size of the
#       "in-memory object data" pool.  This is a pool of 4k pages used
#       to hold object data.
#
#       In-transit objects have priority over the others.  When
#       additional space is needed for incoming data, negative-cached
#       and hot objects will be released.  In other words, the
#       negative-cached and hot objects will fill up any unused space
#       not needed for in-transit objects.
#
#       The values of cache_mem_low and cache_mem_high (below) can be
#       used to tune the use of the memory pool.  When the high mark is
#       reached, in-transit and hot objects will be released to clear
```

```
#       space.  When an object transfer is completed, it will remain in
#       memory only if the current memory usage is below the low water
#       mark.
#
#       The default is 8 Megabytes.
#
cache_mem  8 MB

#  TAG: cache_swap (megabytes)
#       Maximum about of disk space used by the cache.  The default is
#       100 megabytes.  When the disk usage gets to this size, the cache
#       uses LRU replacement to evict objects as new objects are cached.
#       Note that cache_swap is set to:
#               max(cache_mem, cache_swap_specified)
#       to guard against users' accidentally specifying a smaller
#       cache_swap than cache_mem size.
#
#cache_swap 100 MB


#  TAG: cache_swap_low  (percent, 0-100)
#  TAG: cache_swap_high (percent, 0-100)
#       The low- and high-water marks for cache LRU replacement.
#       LRU replacement begins when the high-water mark is reached
#       and ends when enough objects have been removed and the low-water
#       mark is reached. Defaults are 90% and 95%.
#
cache_swap_low  90
cache_swap_high 95

#  TAG: cache_mem_low  (percent, 0-100)
#  TAG: cache_mem_high (percent, 0-100)
#       The low- and high-water mark for cache memory storage.  When
#       the amount of RAM used by the hot-object RAM cache reaches this
#       point, the cache starts throwing objects out of the RAM cache
#       (but they remain on disk).  Defaults are 75% and 90%.
#
#cache_mem_low  75
#cache_mem_high 90

#  TAG: maximum_object_size
#       Objects larger than this size will NOT be saved on disk.  The
#       value is specified in kilobytes, and the default is 4MB.
#
#maximum_object_size 4096

#  TAG: ipcache_size (number of entries)
#  TAG: ipcache_low  (percent)
#  TAG: ipcache_high (percent)
#       The size, low-, and high-water marks for the IP cache.
#
ipcache_size 1024
ipcache_low  90
ipcache_high 95
```

```
# LOGFILE PATHNAMES AND CACHE DIRECTORIES
#-----------------------------------------------------------------------------
--

#  TAG: cache_dir
#       Directory for on-disk cache storage.  The cache will change into
#       this directory when running.  The default is
#       /usr/local/squid/cache.
#
#       You can specify multiple cache_dir lines to spread the
#       cache among different disk partitions.
#
cache_dir /usr/local/squid/cache 100 16 256

#  TAG: cache_access_log
#       Logs the client request activity.  Contains an entry for
#       every HTTP and ICP request received.
#
cache_access_log /usr/local/squid/logs/access.log

#  TAG: cache_log
#       Cache logging file.  Set logging levels with "debug_options" below.
#
cache_log /usr/local/squid/logs/cache.log

#  TAG: cache_store_log
#       Logs the activities of the storage manager.  Shows which
#       objects are ejected from the cache, and which objects are
#       saved and for how long.  To disable, enter "none".
#
cache_store_log /usr/local/squid/logs/store.log

#  TAG: cache_swap_log
#       Location for the cache "swap log."  This log file holds the
#       metadata of objects saved on disk.  It is used to rebuild the
#       cache during startup.  Normally this file resides in the first
#       'cache_dir' directory, but you may specify an alternate
#       pathname here.  Note you must give a full filename, not just
#       a directory.
#
#cache_swap_log /usr/local/squid/cache

#  TAG: emulate_httpd_log
#       The Cache can emulate the log file format which many 'httpd'
#       programs use.  To disable/enable this emulation, set
#       emulate_httpd_log to 'off' or 'on'.  The default
#       is to use the native log format.
#
emulate_httpd_log off

#  TAG: log_mime_hdrs
#       The Cache can record both the request and the response
#       MIME headers for each HTTP transaction.  The headers are
#       encoded safely and will appear as two bracketed fields
```

```
#       at the end of the access log (for either the native
#       or httpd-emulated log formats).  To enable this logging
#       set log_mime_hdrs to 'on'.
#
#       NOTE: support for this may require you to define
#       LOG_FULL_HEADERS before compiling.
#
#log_mime_hdrs off

#  TAG: useragent_log
#       If compiled with "-DUSE_USERAGENT_LOG=1" Squid will write
#       the User-Agent field from HTTP requests to the filename
#       specified here.  By default useragent_log is disabled.
#
#useragent_log none

#  TAG: pid_filename
#       A pathname to write the process-id to.  To disable, enter "none".
#
pid_filename /usr/local/squid/logs/squid.pid

#  TAG: debug_options
#       Logging options are set as section,level where each source file
#       is assigned a unique section.  Lower levels result in less
#       output,  Full debugging (level 9) can result in a very large
#       log file, so be careful.  The magic word "ALL" sets debugging
#       levels for all sections.  We recommend normally running with
#       "ALL,1".
#
#debug_options ALL,1

#  TAG: ident_lookup
#       If you wish to make an RFC931/ident lookup of the client username
#       for each connection, enable this.  It is off by default.
#
#ident_lookup off

#  TAG: log_fqdn
#       Turn this on if you wish to log fully qualified domain names
#       in the access.log.
#
log_fqdn off

#  TAG: client_netmask
#       A netmask for client addresses in logfiles and cachemgr output.
#       Change this to protect the privacy of your cache clients.
#
#client_netmask 255.255.255.0


# OPTIONS FOR EXTERNAL SUPPORT PROGRAMS
#-----------------------------------------------------------------------------
--

#  TAG: ftpget_program
```

```
#       Where to find the 'ftpget' program that retrieves FTP data (HTTP
#       and Gopher protocol support are built into the cache).
#
#       To disable ftpget and the ability to retrieve FTP objects, set
#       this to "none".  Note that ftpget is automatically disabled for
#       http_accel mode.
#
#ftpget_program /usr/local/squid/bin/ftpget

#  TAG: ftpget_options
#       Options for the 'ftpget' program.  Please run 'ftpget' without
#       any arguments to see a list of options.  The default is
#       no options.  An example is
#
#       ftpget_options -n 60 -R -W
#
#ftpget_options

# If you want the anonymous login password to be more informative
# (and enable the use of picky ftp servers), set this to something
# resonable for your domain, like wwwuser@somewhere.net
#
# The reason why this is domainless by default is that the
# request can be made on the behalf of a user in any domain,
# depending on how the cache is used.
# Some ftp server also validate that the email address is valid
# (for example perl.com).
#
ftp_user ftpuser_name@

#  TAG: cache_dns_program
#       Specify the location of the executable for dnslookup process.
#
#cache_dns_program /usr/local/squid/bin/dnsserver

#  TAG: dns_children
#       The number of processes spawn to service DNS name lookups.
#       For heavily loaded caches on large servers, you should
#       probably increase this value to at least 10.  The maximum
#       is 32.  The default is 5.
#
#       To disable dnsservers, set this to 0.  NOTE, this is very
#       strongly discouraged.  If you disable dnsservers your Squid
#       process will BLOCK on DNS lookups!
#
#dns_children 5

#  TAG: dns_defnames
#       Normally the 'dnsserver' disables the RES_DEFNAMES resolver
#       option (see res_init(3)).  This prevents caches in a hierarchy
#       from interpreting single-component hostnames locally.  To allow
#       dnsserver to handle single-component names, enable this
#       option.
#
#dns_defnames off
```

```
#  TAG: unlinkd_program
#       Specify the location of the executable for file deletion process.
#
#unlinkd_program /usr/local/squid/bin/unlinkd

#  TAG: pinger_program
#       Specify the location of the executable for the pinger process.
#
#pinger_program /usr/local/squid/bin/pinger

#  TAG: redirect_program
#       Specify the location of the executable for the URL redirector.
#       Currently, you must provide your own redirector program.
#       See the Release-Notes for how to write one.
#       By default, the redirector is not used.
#
#redirect_program /bin/false

#  TAG: redirect_children
#       The number of redirector processes to spawn.
#
#redirect_children 5


# OPTIONS FOR TUNING THE CACHE
#-----------------------------------------------------------------------------
--

#  TAG: wais_relay
#       Relay WAIS request to host (1st arg) at port (2 arg).
#
#wais_relay localhost 8000

#  TAG: request_size
#       Maximum allowed request size in kilobytes.  If people are using
#       POST to upload files, then set this to the largest acceptable
#       filesize plus a few extra kbytes.
#
#request_size 150

#  TAG: refresh_pattern         # case sensitive
#  TAG: refresh_pattern/i       # case insensitive
#
#       usage: refresh_pattern regex min percent max
#
#       min and max are specified in MINUTES.
#       percent is an integer number.
#
#       Please see the file doc/Release-Notes-1.1.txt for a full
#       description of Squid's refresh algorithm.  Basically a
#       cached object is:
#
#               FRESH if age < min
#               STALE if expires < now
#               STALE if age > max
#               FRESH if lm-factor < percent
```

```
#
#       The refresh_pattern lines are checked in the order listed here.
#       The first entry which matches is used.  If none of the entries
#       match, then the default will be used.
#
#Default:
refresh_pattern         .       0 20% 4320

#  TAG: reference_age
#       As a part of normal operation, Squid performs Least Recently
#       Used removal of cached objects.  The LRU age for removal is
#       computed dynamically, based on the amount of disk space in
#       use.  The 'reference_age' value defines the maximum LRU age.
#       For example, setting reference_age to '1 week' will cause
#       objects to be removed if they have not been accessed for a week
#       or more.  If set to zero, LRU removal is disabled, and objects
#       will be removed only when disk usage is over the high water
#       mark.  The default value is one year.
#
#       Specify a number here, followed by units of time.  For example:
#               1 week
#               3.5 days
#               4 months
#               2.2 hours
#
reference_age 1 year

#  TAG: quick_abort
#       By default the cache continues to retrieve objects from
#       aborted requests.  This may be undesirable on slow (e.g. SLIP)
#       links and/or very busy caches.  Impatient users may tie up
#       file descriptors by repeatedly aborting and re-requesting
#       non-cachable objects.
#
#       Usage: quick_abort    min-kbytes percent max-kbytes
#
#       When the user aborts a request, Squid will check the
#       quick_abort values to the amount of data transfered until
#       then.
#
#       If the transfer has less than 'min-kbytes' remaining, it
#       will finish the retrieval.  Setting minlength to -1 will
#       disable the quick_abort feature.
#
#       If the transfer has more than 'max-kbytes' remaining, it
#       will abort the retrieval.
#
#       If more than 'percent' of the transfer has completed, it will
#       finish the retrieval.
#
#quick_abort    min percent max

#  TAG: negative_ttl (minutes)
#       Time-to-Live (TTL) for failed requests.  Certain types of
#       failures (such as "connection refused" and "404 Not Found") are
#       negatively-cached for a small amount of time.  The default is 5
#       minutes.  Note that this is different from negative caching of
#       DNS lookups.
```

```
#
#negative_ttl 5

#
#  TAG: positive_dns_ttl (minutes)
#       Time-to-Live (TTL) for positive caching of successful DNS lookups.
#       Default is 6 hours (360 minutes).  If you want to minimize the
#       use of Squid's ipcache, set this to 1, not 0.
#
#positive_dns_ttl 360

#  TAG: negative_dns_ttl (minutes)
#       Time-to-Live (TTL) for negative caching of failed DNS lookups.
#
#negative_dns_ttl 5


# TIMEOUTS
#-----------------------------------------------------------------------------
--

#  TAG: connect_timeout (seconds)
#       Some systems (notably Linux) can not be relied upon to properly
#       time out connect(2) requests.  Therefore the squid process
#       enforces its own timeout on server connections.  This parameter
#       specifies how long to wait for the connect to complete.  The
#       default is two minutes (120 seconds).
#
#connect_timeout 120

#  TAG: read_timeout (minutes)
#       An active connection will be aborted after read_timeout minutes
#       of no activity on that connection (i.e., assume the remote server
#       or network connection died after the connection was established).
#       The default is 15 minutes.
#
#read_timeout 15

#  TAG: client_lifetime (minutes)
#       The maximum amount of time that a client (browser) is allowed to
#       remain connected to the cache process.  This protects the Cache
#       from having alot of sockets (and hence file descriptors) tied up
#       in a CLOSE_WAIT state from remote clients that go away without
#       properly shutting down (either because of a network failure or
#       because of a poor client implementation).  The default is three
#       hours, 20 minutes.
#
#       NOTE:  The default value is designed with low-speed client
#       connections in mind.  200 minutes should be plenty of time to
#       transfer a 10M file at 1k/sec.  If you have high-speed client
#       connectivity, or occasionally run out of file descriptors,
#       we suggest you lower this value appropriately.
#
#client_lifetime 200
```

```
#  TAG: shutdown_lifetime (seconds)
#
#       When SIGTERM or SIGHUP is received, the cache is put into
#       "shutdown pending" mode until all active sockets are closed.
#       This value is the lifetime to set for all open descriptors
#       during shutdown mode.  Any active clients after this many
#       seconds will receive a 'lifetime expire' message
#
#shutdown_lifetime 30

# ACCESS CONTROLS
#-----------------------------------------------------------------------------
--

# Defining an Access List
#
# acl aclname acltype string1 ...
# acl aclname acltype "file" ...
#
# when using "file", the file should contain one item per line
#
# acltype is one of src dst srcdomain dstdomain url_pattern urlpath_pattern
#                    time port proto method browser user
#
# acl aclname src      ip-address/netmask ... (clients IP address)
# acl aclname src      ip-address/netmask ... (clients IP address)
# acl aclname src      addr1-addr2/netmask ... (range of addresses)
# acl aclname dst      ip-address/netmask ... (URL host's IP address)
# acl aclname srcdomain   foo.com ... (taken from reverse DNS lookup)
# acl aclname dstdomain   foo.com ... (taken from the URL)
# acl aclname time     [day-abbrevs]  [h1:m1-h2:m2]
#       day-abbrevs:
#               S - Sunday
#               M - Monday
#               T - Tuesday
#               W - Wednesday
#               H - Thursday
#               F - Friday
#               A - Saturday
#       h1:m1 must be less than h2:m2
# acl aclname url_regex  ^http:// ...   # regex matching on whole URL
# acl aclname urlpath_regex  \.gif$ ... # regex matching on URL path only
# acl aclname port     80 70 21 ...
# acl aclname proto    HTTP FTP ...
# acl aclname method   GET POST ...
# acl aclname browser  regexp
# acl aclname user     username ...     # string match on ident output.
#                                       # use REQUIRED to accept any
#                                       # non-null ident.

acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
acl inside src 192.168.1.0/255.255.255.0
acl inside src 192.168.1.0/255.255.255.0
```

```
acl example src 192.168.1.113/255.255.255.255
acl SSL_ports port 443 563
acl Dangerous_ports port 7 9 19
acl CONNECT method CONNECT

# Allowing or Denying access based on defined access lists
#
# Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
# Access to the ICP port:
#     icp_access  allow|deny [!]aclname ...
#
# NOTE on default values:
#
#       If there are no "access" lines present, the default is to allow
#       the request.
#
#       If none of the "access" lines cause a match, the default is the
#       opposite of the last line in the list.  If the last line was
#       deny, then the default is allow.  Conversely, if the last line
#       is allow, the default will be deny.  For these reasons, it is a
#       good idea to have an "deny all" or "allow all" entry at the end
#       of your access lists to avoid potential confusion.


# Only allow access to the cache manager functions from the local host.
#http_access deny manager !localhost
http_access allow manager localhost
http_access deny manager
http_access deny CONNECT !SSL_ports
http_access deny CONNECT !SSL_ports
http_access deny CONNECT !SSL_ports
http_access deny Dangerous_ports
#http_access allow localclients
http_access allow manager example
# Allow everything else
http_access allow inside
http_access allow localhost
http_access allow all
#http_access allow localclients

# Reply to all ICP queries we receive
icp_access  deny  all
#icp_access  allow localclients

#  TAG: miss_access
#       Use to force your neighbors to use you as a sibling instead of
#       a parent.  For example:
#
#               acl localclients src 172.16.0.0/16
#               miss_access allow localclients
#               miss_access deny  !localclients
#
#       This means that only your local clients are allowed to fetch
```

```
#       MISSES and all other clients can only fetch HITS.
#
#       By default, allow all clients who passed the http_access rules
#       to fetch MISSES from us.
#
miss_access allow  all
miss_access allow manager
#  TAG: cache_host_acl
#       Just like 'cache_host_domain' but provides more flexibility by
#       using ACL's.
#
#               cache_host_acl cache-host       [!]aclname ...
#
#       NOTE:   * Any number of ACL's may be given for a cache-host,
#                 either on the same or separate lines.
#               * When multiple ACL's are given for a particular
#                 cache-host, the first matched ACL is applied.
#               * Cache hosts with no domain or ACL restrictions are
#                 queried for all requests.
#               * There are no defaults.


# ADMINISTRATIVE PARAMETERS
#-----------------------------------------------------------------------------
--

#  TAG: cache_mgr
#       Email-address of local cache manager who will receive
#       mail if the cache dies.  The default is "webmaster."
#
cache_mgr iclab-admin

#  TAG: cache_effective_user
#       If the cache is run as root, it will change its effective/real
#       UID/GID to the UID/GID specified below.  The default is not to
#       change UID/GID.
#
#cache_effective_user nobody nogroup
cache_effective_user andree staff


#  TAG: visible_hostname
#       If you want to present a special hostname in error messages, etc,
#       then define this.  Otherwise, the return value of gethostname()
#       will be used.
#
#visible_hostname www-cache.foo.org


# OPTIONS FOR THE CACHE REGISTRATION SERVICE
#-----------------------------------------------------------------------------
--

#       This section contains parameters for the (optional) cache
#       announcement service.  This service is provided to help
```

```
#       cache administrators locate one another in order to join or
#       create cache hierarchies.
#
#       An 'announcement' message is sent (via UDP) to the registration
#       service by Squid.  By default, the annoucement message is NOT
#       SENT unless you enable it with 'cache_announce' below.
#
#       The announcement message includes your hostname, plus the
#       following information from this configuration file:
#
#               http_port
#               icp_port
#               cache_mgr
#
#       All current information is processed regularly and made
#       available on the Web at http://www.nlanr.net/Cache/Tracker/.


# This is how frequently to send cache announcements.  The default
# is `0' which disables sending the announcement messages.
#
# To enable announcing your cache, just uncomment the line below.
#
#cache_announce 24

# This is the hostname and portnumber where the registration message
# will be sent.
#
# Format:       announce_to   host[:port] [filename]
#
# Hostname will default to 'tracker.ircache.net' and port will default
# to 3131.  If the 'filename' argument is given, the contents of that
# file will be included in the announce message.
#
#announce_to tracker.ircache.net:3131


# HTTPD-ACCELERATOR OPTIONS
#-----------------------------------------------------------------------------
--

#  TAG: httpd_accel
#       If you want to run squid as an httpd accelerator, define the
#       host name and port number where the real HTTP server is.
#
#       If you want virtual host support then specify the hostname
#       as "virtual".
#
#httpd_accel real_httpd_host real_httpd_port

#  TAG: httpd_accel_with_proxy
#       If you want to use squid as both a local httpd accelerator
#       and as a proxy, change this to 'on'.
#
#httpd_accel_with_proxy off
```

```
#  TAG: httpd_accel_uses_host_header
#       HTTP/1.1 requests include a Host: header which is basically the
#       hostname from the URL.  Squid can be an accelerator for
#       different HTTP servers by looking at this header.  However,
#       Squid does NOT check the value of the Host header, so it opens
#       a big security hole.  We recommend that this option remain
#       disabled unless you are sure of what you are doing.
#
#httpd_accel_uses_host_header off


# MISCELLANEOUS
#---------------------------------------------------------------------------
--

# The DNS tests exit as soon as the first site is successfully looked up
#
# If you want to disable DNS tests, do not comment out or delete this
# list.  Instead use the -D command line option
#
dns_testnames internic.net usc.edu cs.colorado.edu mit.edu yale.edu

#  TAG: logfile_rotate #
#       Specifies the number of logfile rotations to make upon receiving
#       a USR1 signal.  The default is 10, which will rotate with
#       extensions 0 through 9.  Setting logfile_rotate to 0 will
#       disable the rotation, but the logfiles are still closed and
#       re-opened.  This will enable you to rename the logfiles yourself
#       just before sending a USR1 signal to the squid process.
#
logfile_rotate 10

#  TAG: append_domain
#       Appends local domain name to hostnames without any dots in them.
#       append_domain must begin with a period.
#
#append_domain .ce.nihon-u.ac.jp

#  TAG: tcp_recv_bufsize
#       Size of receive buffer to set for TCP sockets.  Probably just
#       as easy to change your kernel's default.  Set to zero to use
#       the default buffer size.
#
#tcp_recv_bufsize 0


#  TAG: ssl_proxy
#       Specify the name of a 'cache_host' listed above, or a hostname
#       and port number where all SSL requests should be forwarded to.
#
#       Usage: ssl_proxy cache_host
#              ssl_proxy host:port
#
#ssl_proxy
```

```
#  TAG: passthrough_proxy
#       Specify the name of a 'cache_host' listed above, or a hostname
#       and port number where all non-GET (i.e. POST, PUT) requests
#       should be forwarded to.
#
#       Usage: passthrough_proxy cache_host
#              passthrough_proxy host:port
#
#passthrough_proxy

#  TAG: proxy_auth
#       Usage: proxy_auth passwd_file [ ignore-domain ]
#
#       'passwd_file' is an apache-style file of passwords for
#       authenticated proxy access Looks like user:password, with the
#       password being standard crypt() format.  Proxy authentication
#       is disabled by default.
#
#       'ignore-domain' is a domain name for which authorization will
#       *not* be required.
#
#       NOTE, proxy_auth support is not compiled into Squid by default.
#       To use this feature you must enable the USE_PROXY_AUTH option
#       near the top of src/Makefile.
#
#proxy_auth /dev/null

#  TAG: err_html_text
#       HTML text to include in error messages.  Make this a "mailto"
#       URL to your admin address, or maybe just a link to your
#       organizations Web page.
#
#err_html_text

#  TAG: deny_info
#       Usage: deny_info URL acl
#
#       This can be used to return a HTTP redirect for requests which
#       do not pass the 'http_access' rules.  A single ACL will cause
#       the http_access check to fail.  If a 'deny_info' line exists
#       for that ACL then Squid returns a redirect to the given URL.

#  TAG: udp_hit_obj on|off
#       If set, Squid will request UDP_HIT_OBJ replies from its
#       neighbors.  UDP_HIT_OBJ is nice because it saves bandwidth, but
#       it can cause some other problems.  For one it complicates
#       calculating hit rates.  Also, problems arise because the ICP
#       query does not contain any HTTP request headers which may
#       affect the reply.
#
#udp_hit_obj off

#  TAG: udp_hit_obj_size
#
```

```
#     If set, Squid will limit UDP_HIT_OBJ size to be less than
#     this value.  Setting this value to more than SQUID_UDP_SO_SNDBUF
#     will not work as expected.  Set to zero to select the size
#     permited by the socket.
#udp_hit_obj_size     0

#  TAG: memory_pools on|off
#       If set, Squid will keep pools of allocated (but unused) memory
#       available for future use.  If memory is a premium on your
#       system, disable this.
#
#memory_pools on

#  TAG: forwarded_for on|off
#       If set, Squid will include your system's IP address or name
#       in the HTTP requests it forwards.  By default it looks like
#       this:
#
#               X-Forwarded-For: 192.1.2.3
#
#       If you disable this, it will appear as
#
#               X-Forwarded-For: unknown
#
#forwarded_for on

#  TAG: log_icp_queries on|off
#       If set, ICP queries are logged to access.log.  ICP logging
#       is enabled by default, so uncomment and change the line
#       below to disable it.
#
#log_icp_queries on


#  TAG: minimum_direct_hops
#       If using the ICMP pinging stuff, do direct fetches for sites
#       which are no more than this many hops away.
#
minimum_direct_hops 4

#  TAG: cachemgr_passwd
#       Specify passwords for cachemgr operations.
#
#Usage: cachemgr_passwd password action action ...
#
#       valid actions are:
#               shutdown *
#               info
#               stats/objects
#               stats/vm_objects
#               stats/utilization
#               stats/ipcache
#               stats/fqdncache
#               stats/dns
#               stats/redirector
```

```
#               stats/io
#               stats/reply_headers
#               stats/filedescriptors
#               stats/netdb
#               log/status *
#               log/enable *
#               log/disable *
#               log/clear *
#               log *
#               parameter
#               server_list
#               client_list
#               squid.conf *
#
#       * Indicates actions which will not be performed without a
#         valid password, others can be performed if not listed here.
#
#       To disable an action, set the password to "disable".
#       To allow performing an action without a password, set the
#       password to "none".
#
#       Use the keyword "all" to set the same password for all actions.
#
#Examples:
#
#       cachemgr_passwd secret shutdown
#       cachemgr_passwd lesssssssecret info stats/objects
#       cachemgr_passwd disable all
#
#Defaults: none

#  TAG: swap_level1_dirs
#       Number of first-level directories to create for storing cached
#       objects.  Minimum 1, maximum 256, default 16.
#
#swap_level1_dirs 16

#  TAG: swap_level2_dirs
#       Number of sub-directories to create under each first-level
#       directory.  Minimum 1, maximum 256, default 256.
#
#swap_level2_dirs 256

#  TAG: store_avg_object_size
#       Average object size, used to estimate number of objects your
#       cache can hold.  See doc/Release-Notes-1.1.txt.  The default is
#       13K.
#
#store_avg_object_size 13

#  TAG: store_objects_per_bucket
#       Target number of objects per bucket in the store hash table.
#       Lowering this value increases the total number of buckets and
#       also the storage maintenance rate.  The default is 20.
#
```

```
#store_objects_per_bucket 20

#  TAG: http_anonymizer
#       If you want to filter out certain HTTP request headers for
#       privacy reasons, enable this option.  There are three
#       appropriate settings:
#               'off'           All HTTP request headers are passed.
#               'standard'      Specific headers are removed
#               'paranoid'      Only specific headers are allowed.
#       To see which headers are allowed or denied, please see the
#       http-anon.c source file.
#
#http_anonymizer off

#  TAG: fake_user_agent
#       If you use the paranoid http_anonymizer setting, Squid will strip
#       your User-agent string from the request.  Some Web servers will
#       refuse your request without a User-agent string.  Use this to
#       fake one up.  For example:
#
#       fake_user_agent Nutscrape/1.0 (CP/M; 8-bit)
#       (credit to Paul Southworth pauls@etext.org for this one!)
#
#fake_user_agent none

#  TAG: client_db
#       If you want to disable collecting per-client statistics, then
#       turn off client_db here.
#
#client_db on

#  TAG: netdb_low
#  TAG: netdb_high
#       The low and high water marks for the ICMP measurement
#       database.  These are counts, not percents.  The defaults are
#       900 and 1000.  When the high water mark is reached, database
#       entries will be deleted until the low mark is reached.
#
#netdb_low 900
#netdb_high 1000

#  TAG: netdb_ping_rate
#       The minimum period for measuring a site.  There will be at
#       least this much delay between successive pings to the same
#       network.  The default is five minutes.
#
#netdb_ping_period 5 minutes

#  TAG: query_icmp
#       If you want to ask your peers to include ICMP data in their ICP
#       replies, enable this option.
#
#       If your peer has built squid with '-DUSE_ICMP=1' then that peer
#       will send ICMP pings to origin server sites of the URLs it
#       receives.  If you enable this option then the ICP replies from
#       that peer will include the ICMP data (if available).  Then,
#       when choosing a parent cache, Squid will choose the parent with
```

```
#       the minimal RTT to the origin server.  When this happens, the
#       hierarchy field of the access.log will be
#       "CLOSEST_PARENT_MISS".  This option is off by default.
#
#query_icmp off

#  TAG: icp_hit_stale
#       If you want to return ICP_HIT for stale cache objects, set this
#       option to 'on'.  If you have sibling relationships with caches
#       in other administrative domains, this should be 'off'.  If you only
#       have sibling relationships with caches under your control, then
#       it is probably okay to set this to 'on'.  NEVER enable
#       icp_hit_stale if you also use 'miss_access'.
#
#icp_hit_stale off

#  TAG: minimum_retry_timeout (Mike Pelletier )
#       This specifies the minimum connect timeout for the retry
#       patch, for instances when the connect timeout is reduced
#       to compensate for the availability of multiple IP addresses.
#
#       When a connection to a host is initiated, and that host has
#       several IP addresses, the default connection timeout is
#       reduced by dividing it by the number of addresses.  So,
#       a site with 15 addresses would then have a timeout of 8
#       seconds for each address attempted.  To avoid having the
#       timeout reduced to the point where even a working host
#       would not have a chance to respond, this setting is
#       provided. The default, and the minimum value, is five
#       seconds, and the maximum value is sixty seconds, or half of
#       connect_timeout, whichever is greater and less than
#       connect_timeout.  This feature is not compiled in by
#       default.  You must add -DRETRY_PATCH in src/Makefile.
#
#minimum_retry_timeout 5

#  TAG: maximum_single_addr_tries
#       This sets the maximum number of connection attempts for a
#       host that only has one address (for multiple-address hosts,
#       each address is tried once) for the retry patch.
#
#       The default value is three tries, the (not recommended)
#       maximum is 255 tries.  A warning message will be generated if
#       it is set to a value greater than ten.  You must add
#       -DRETRY_PATCH in src/Makefile.
#
#maximum_single_addr_tries 3

#  TAG: reload_into_ims
#       Enable this if you want to turn 'Pragma: no-cache' requests
#       into If-Modified-Since requests.  Off by default, use at your
#       own risk.  This feature is not compiled in by default.  You
#       must add -DRELOAD_INTO_IMS in src/Makefile.
#
#reload_into_ims off
#Original design: Andree Toonk! 26-04-2000
```

Index

Figurenlijst

Literatuur

- Telemark Systems, Inc.; "NT DNS Configuration - using BIND 4.9.3 Release"; Telemark Systems, Inc., april 1996; http://www.telemark.net/~randallg/ntdns.htm.
- Langfeldt, Nicolai <janl@math.uio.no>; "DNS-HOWTO" (Linux HowTo); Langfeldt, Nicolai, 1995-1999; http://metalab.unc.edu/pub/linux/docs/howto/DNS-HOWTO.

Datum : 15 juni 2000
Versie : 20000615.01

Documentnr.: 995047

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel VI, Beveiliging en veiligheidsmaatregelen

Indeling van dit document

Hoofdstuk 1 geeft inzicht in beveiliging in het algemeen, wat u kunt doen in het geval dat u vermoedt dat er een beveiligingsprobleem is, en wat u kunt doen om beveiligingsproblemen te voorkomen.

In Hoofdstuk 2 wordt de situatie op kennisnet, en worden de genomen beveiligingsmaatregelen nader toegelicht: hoe is kennisnet beveiligd en hoe veilig is kennisnet?

Inhoudsopgave

Hoofdstuk 1. Beveiliging en veiligheidsprocedures

[Informatie en inspiratie voor dit hoofdstuk is o.a. afkomstig uit de 'Computer Forensics Class 1999' van Wietse Veenema en Dan Farmer: http://www.fish.com/forensics.]

Het is op kennisnet van het grootste belang dat de veiligheid van uw computers en werkstations is gewaarborgd. Hiertoe zijn en worden, voorzover dit mogelijk is, op basis van door het Ministerie van Onderwijs, Wetenschappen en Cultuur vastgestelde richtlijnen en algemeen gebruikte werkwijzen ('common practice') maatregelen genomen.

Het landelijke netwerk wordt beschermd door middel van een firewall die slechts dát verkeer doorlaat, dat expliciet is toegestaan. Routers van schoolnetwerken zijn voorzien van extra beveiligingsregels die selectief netwerkverkeer doorlaten of blokkeren.

Gezien de enorme omvang die kennisnet zal aannemen, en gezien het feit dat er vrij regelmatig beveiligingsfouten in systeemsoftware worden ontdekt en gepubliceerd, is het niet uit te sluiten dat zich, ondanks alle maatregelen, incidenten voordoen. Binnen kennisnet is daarom voorzien in een team dat kan adviseren en assisteren bij het analyseren van veiligheidsincidenten. Voorzover dit – technisch, organisatorisch en wettelijk – in de macht van dit team ligt, zullen waar nodig maatregelen worden genomen.

Het aanspreekpunt voor veiligheidsincidenten is het Servicepunt kennisnet (zie Bijlage A.). Bij het Servicepunt kennisnet heeft men formulieren beschikbaar alsook de juiste contacten om een afdoende rapportage van het incident te maken en de juiste instanties in te schakelen.

1.1 Wat te doen in het geval van een veiligheidsincident?

Heel belangrijk is valide en volledige **informatie**. Deze informatie kan voortkomen uit logbestanden, systeeminformatiesoftware, hulpmiddelen, handleidingen etc. Veel informatie – met name logbestanden en informatie geproduceerd door systeeminformatiesoftware (netwerkstatus, actieve processen e.d. – dient te worden voorzien van datum en tijd. Minstens zo belangrijk is, dat deze tijd *correct* is en voorzien van de juiste tijdzoneaanduiding. Het is derhalve aan te raden om voor uw belangrijke servers gebruik te maken van een tijdserver (zie deel III).

Indien u het vermoeden hebt dat een systeem op uw netwerk is of wordt aangevallen, probeer dan om zoveel mogelijk informatie veilig te stellen en, indien mogelijk, de bron van de aanval te achterhalen. Controleer hiertoe actieve netwerkverbindingen en -sessies.

Onder Windows kunt u met het commando 'netstat' informatie krijgen over openstaande IP-sessies. Met de optie '-a' krijgt u *alle* open verbindingen te zien. Door de optie '-n' mee te geven, ziet u alleen een numerieke weergave die voorkomt dat er een DNS-controle wordt gedaan, welke het beeld bovendien kan verstoren.

Voorbeeld:

```
C:\> netstat -a -n
```

Geef de optie '/?' om meer informatie over dit commando te krijgen.

Onder UNIX/Linux kunt u met het commando 'netstat' informatie krijgen over openstaande IP-sessies. Met de optie '-a' krijgt u *alle* open verbindingen te zien. Door de optie '-n' mee te geven, ziet u alleen een numerieke weergave die voorkomt dat er een DNS-controle wordt gedaan, welke het beeld bovendien kan verstoren.

Voorbeeld:

```
$ netstat -an
```

Geef de optie '--help' of gebruik 'man netstat' om meer informatie over dit commando te krijgen.

Stel *alle* logbestanden die u kunt vinden, zo snel mogelijk veilig op een extern opslagmedium of een ander computersysteem. Op UNIX-systemen kunt u de logbestanden meestal vinden in de map `/var/log` of `/var/logs`.

Ontkoppel indien mogelijk of indien noodzakelijk (welk van de twee zwaarder weegt, dient voorrang te krijgen) het betreffende systeem van het netwerk door eenvoudig de netwerkkabel te ontkoppelen. Dit *kan*, indien het een geval van ‘heterdaad’ betreft, de opsporing van de dader bemoeilijken of onmogelijk maken.

Belangrijk is nu om het systeem zoveel mogelijk te laten zoals het is voor nadere analyse. Let op dat *elke* handeling die u uitvoert, invloed kan hebben op de status van het systeem en onderdelen ervan. Idealiter zou u het systeem moeten 'bevriezen', zodat het geheugen, de disk- en geheugenbuffers (caches) en de status van de harde schijf onveranderd blijven. Advanced Power Management kan hierbij behulpzaam zijn, doordat sommige systemen in staat zijn om het geheugen naar een speciale partitie op de harde schijf weg te schrijven en zo de status van het systeem vast te leggen. Helaas betreft dit voornamelijk laptop-computers en slechts sporadisch servers. Maak vooral, indien Advanced Power Management geen uitkomst kan bieden, een volledige back-up van uw systeem.

Neem contact op met het Servicepunt kennisnet om het incident te melden. Het Servicepunt kennisnet kan contact opnemen met de juiste instanties. Neem tevens contact op met uw netwerkleverancier en/of -beheerpartij om na te gaan welke mogelijkheden men heeft om het incident te analyseren en schade te herstellen.

In het geval dat uw systeem getroffen wordt door een 'Trojaans paard'[1], dient u er rekening mee te houden dat de enige remedie is om uw systeem van de grond af op te bouwen met behulp van de installatiediskettes of CD-ROM's. Trojaanse paarden kunnen geruime tijd op uw systeem actief zijn voordat ze toeslaan! Als u geluk hebt, kunt u de grootste schade herstellen door back-ups van enkele maanden oud terug te zetten.

1.2 Ik heb het vermoeden dat er op mijn systeem is of wordt ingebroken. Wat moet ik doen?

Raak niet in paniek, maar probeer zoveel mogelijk gegevens over het incident te verzamelen en veilig te stellen. Doe dit zoveel mogelijk zonder dat de 'inbreker' hier iets van merkt. Licht het Servicepunt kennisnet in en probeer daarbij zoveel mogelijk relevante informatie te verstrekken.

Ontkoppel indien mogelijk of indien noodzakelijk (welk van de twee zwaarder weegt, dient voorrang te krijgen) het betreffende systeem van het netwerk door eenvoudig de netwerkkabel te ontkoppelen. Dit *kan*, indien het een geval van ‘heterdaad’ betreft, de opsporing van de dader bemoeilijken of onmogelijk maken.

Voordat u een incident rapporteert, dient u er rekening mee te houden dat de ‘aanval’ géén inbraak betreft, maar mogelijk een softwarefout of een computervirus. Probeer na te gaan of dit tot de mogelijkheden behoort vóór u een mogelijk vals alarm meldt. Wacht ook niet te lang met melden: heel misschien is het mogelijk de dader op heterdaad te betrappen.

Als er echter daadwerkelijk iets aan de hand is, kan het beveiligingsteam van nl.tree worden ingeschakeld en u ter zijde staan. U kunt het beveiligingsteam bereiken via het Servicepunt kennisnet (0800-KENNISNET/0800-536647638), keuze 3, of per e-mail via '`security@kennisnet.nl`'.



[1] 'Trojan Horse', naar analogie van de legende van het paard van Troje: een type computervirus, dat zich via een op zichzelf onschuldig lijkend programma in uw systeem nestelt en vrij onverwacht toeslaat.

1.3 Er is een 'portscan' uitgevoerd op mijn netwerk. Is dat erg?

Ja en nee. Om met 'nee' te beginnen: op zich kan een portscan geen kwaad. Er wordt slechts kortstondig getracht een verbinding op te zetten en direct weer verbroken. Er wordt dus niet ingebroken of getracht aan te melden onder valse voorwendselen.

Maar ook het 'ja'-antwoord dient gegeven te worden, omdat het soms betekent dat iemand probeert om bijvoorbeeld gevoelige systemen en netwerkdiensten te vinden. Lang niet altijd is een portscan kwaadaardig bedoeld, maar dat kan inderdaad wel het geval zijn.

Waar u op moet letten, is welke poorten gescand zijn en of dit mogelijk 'bijzondere' poorten zijn, die door 'hacker-tools' gebruikt kunnen worden of die bij applicaties horen waarvan recent beveiligingsproblemen zijn gemeld.

1.4 Hoe kan ik veiligheidsincidenten en schade voorkomen?

Inderdaad, voorkomen! ‘Voorkomen is beter dan genezen’, is een bekende uitspraak die ook in dit geval van toepassing is. Veel, zo niet de meeste incidenten worden veroorzaakt doordat 'crackers' gebruikmaken van fouten in netwerk- en systeemsoftware. In verband hiermee kunnen de volgende tips worden gegeven.

- Probeer zoveel mogelijk de laatste stabiele versie van netwerk- en systeemsoftware te gebruiken en gebruik de laatste 'patches' ('lapmiddeltjes') die de softwareproducenten beschikbaar stellen, wanneer elders incidenten zijn gerapporteerd met de betreffende software.
- Gebruik waar mogelijk alleen software van betrouwbare bronnen, dus rechtstreeks van uw leverancier of van vertrouwde websites.
- Installeer een virusscanner en neem bij voorkeur een abonnement om regelmatig verse antivirusinformatie te ontvangen van de producent.
- Zorg ervoor dat zo min mogelijk software op uw systemen is geïnstalleerd en geactiveerd. Installeer alleen de software die nodig is voor het normaal functioneren van het systeem, en die nodig is om te bereiken waarvoor het systeem bedoeld is. Activeer alleen die programmatuur, die noodzakelijk is om de diensten die u wilt leveren, daadwerkelijk te kunnen leveren. Onder Windows NT doet u er bijvoorbeeld verstandig aan om alle niet-noodzakelijke 'Network Services' uit te schakelen! Onder RedHat of SuSe Linux kunt u met de 'Runlevel Editor' aangeven welke processen/diensten u bij het opstarten van het systeem wel of niet wilt opstarten.
- Controleer regelmatig of er geen verdachte processen op uw computer actief zijn. Dit kunt u doen door een proceslijst op te vragen[2]. Controleer daarnaast of er geen verdachte netwerkpoorten in gebruik zijn, bijvoorbeeld met het commando 'netstat' onder Windows of UNIX/Linux (zie boven). Dit laatste vergt echter wel enige kennis van netwerksoftware en poortnummers. Een nuttige bron van informatie kan de lijst van 'assigned numbers' zijn:

  http://www.isi.edu/in-notes/iana/assignments/port-numbers.
- Inspecteer met enige regelmaat uw logbestanden op verdachte zaken. Voor bepaalde typen logbestanden en besturingssystemen is analysesoftware beschikbaar. Kijk hiervoor op bijvoorbeeld http://www.tucows.com, http://www.software.com, of http://www.download.com.
- Maak regelmatig, liefst dagelijks, back-ups van uw vitale computersystemen – **ook van uw log- en configuratiebestanden**!
- Laat het onderhoud en beheer van uw systemen eventueel uitvoeren door een gespecialiseerde partij met kennis van zaken omtrent de beveiliging van computersystemen.

[2] Onder Windows 95/98 en NT is de lijst met actieve programma's **niet** voldoende om inzicht te krijgen in de werkelijk actieve software. Hiervoor dient u ten minste een programma als 'Systeeminfo' te draaien.

- Zorg dat u op de hoogte blijft van probleemrapportages van de door u gebruikte software. Dit kunt u doen door zich te abonneren op een zogenaamde mailinglist of nieuwsbrief van bijvoorbeeld een gebruikersgroep of van de producent van de software. Een andere mogelijkheid is om regelmatig websites en/of nieuwsgroepen rond dit onderwerp te raadplegen.
  - http://www.cert.org/advisories/
  - http://www.rootshell.com
  - http://www.insecure.org
  - http://www.ntsecurity.net/

1.5 Wat is het verschil tussen een 'hacker' en een 'cracker'?

Van oudsher is 'hacker' de aanduiding voor iemand die handig is in het schrijven van slimme software en goed met computers overweg kan. Een 'hacker' heeft misschien de mogelijkheid en kennis om systemen te kraken, maar niet de intentie. De term 'hacken' wordt ook wel gebruikt voor (vaak 'even gauw') iets programmeren.

Een 'cracker' daarentegen is een stuk minder onschuldig. Een 'cracker' is ook erg handig, maar gebruikt zijn/haar handigheid om systemen te kraken (in te breken), mogelijk gegevens te stelen, te vernietigen of te corrumperen.

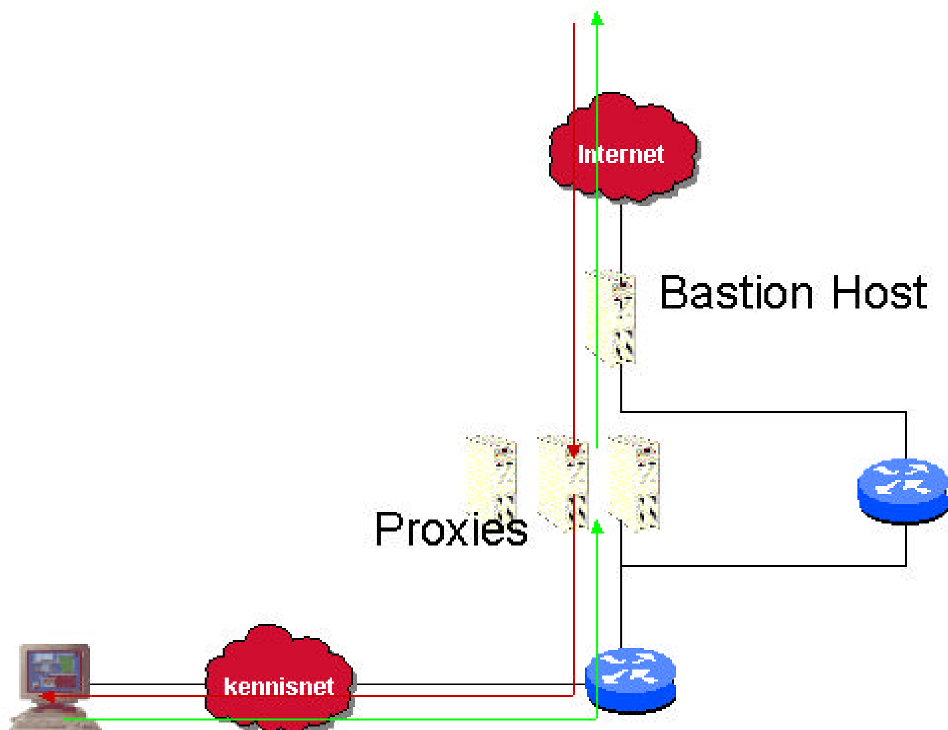
In de volksmond wordt aan de term 'hacker' meestal de betekenis van 'cracker' toegekend.

Hoofdstuk 2. Beveiliging kennisnet

2.1 Hoe is kennisnet beveiligd tegen aanvallen?

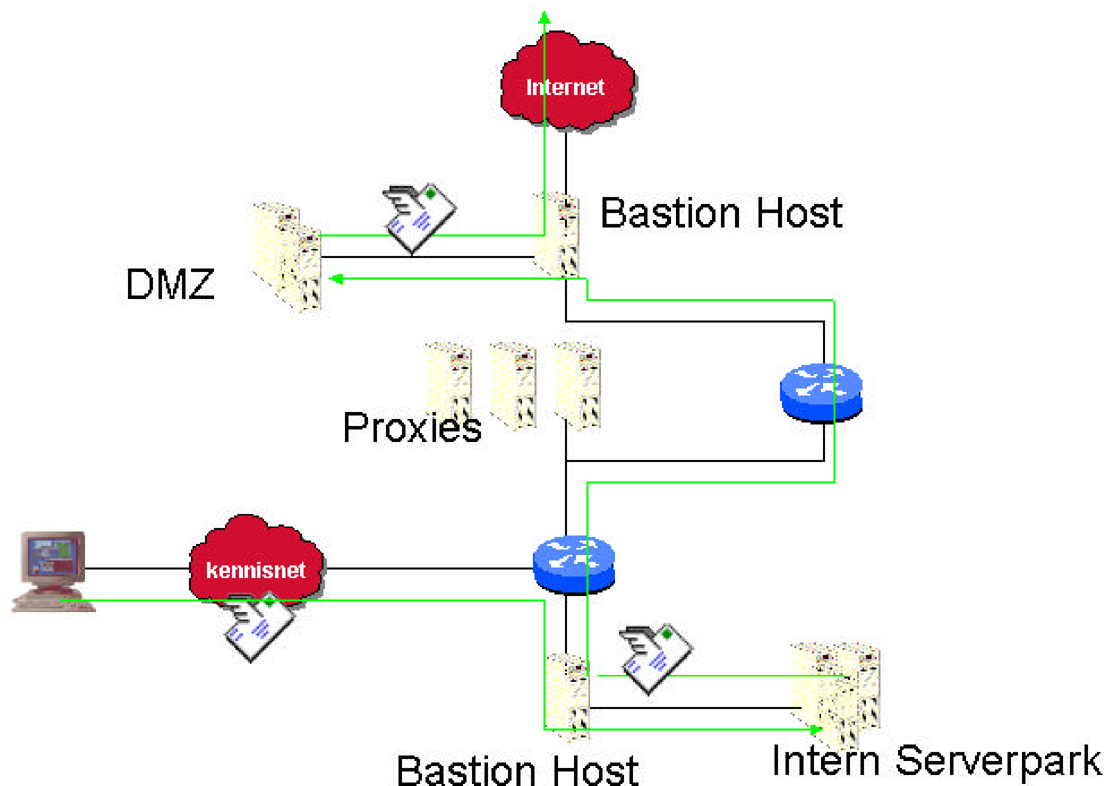
De beveiliging van kennisnet is zo opgezet, dat er géén rechtstreeks verkeer kan lopen van binnen naar buiten, of andersom. Al het verkeer tussen kennisnet en het Internet loopt via proxyservers en relayservers.

De proxyservers zijn bedoeld om toepassingen waarvoor u normaal een rechtstreekse verbinding met de eindbestemming zou opzetten vanuit kennisnet mogelijk te maken. Denk hierbij aan het web, FTP, RealAudio/Video (filmpjes, muziek en radio via het Internet), Telnet en IRC.



Figuur 1: proxystructuur

De relayservers zijn bedoeld voor diensten waarbij niet altijd een rechtstreekse verbinding hoeft te worden opgebouwd met de eindbestemming. E-mail en news worden via-via naar buiten geleid.



Figuur 2: mailrelays

Door deze beveiligingsmaatregelen is het in principe niet mogelijk dat iemand vanaf het Internet rechtstreeks uw systemen of de interne systemen van kennisnet benadert.

2.2 Hoe is mijn schoolaansluiting beveiligd tegen aanvallen?

Uw aansluiting op kennisnet bestaat uit een router en/of kabelmodem. Soms is dit een gecombineerd systeem. In ieder geval bevat uw aansluiting routingfunctionaliteit. De router (zie ook deel I) biedt de mogelijkheid om behalve de weg te wijzen aan voorbijkomend IP-verkeer, ook te selecteren welk verkeer wel en niet van en naar uw lokale netwerk mag.

Binnen kennisnet zijn afspraken gemaakt over een standaardbeveiliging van het schoolnetwerk. In deel I hebt u kunnen zien hoe de IP-reeks is ingedeeld:

- het grootste deel is bedoeld voor werkplekken;
- een deel is bedoeld voor uw servers, die op kennisnet zichtbaar moeten zijn;
- tenslotte is een deel bedoeld voor uw servers en overige apparatuur die **uitsluitend** bereikbaar mogen zijn vanaf uw lokale netwerk.

Voor elk van deze delen geldt een andere manier van filteren. Het filteren geschiedt op basis van het IP-adres (het unieke adres op het Internet) van de systemen en de zogenoemde poortnummers. 'Poorten' worden gebruikt door applicaties om de verbindingen te identificeren. Bepaalde applicaties hebben voor inkomend verkeer een vast poortnummer – web: poort 80; e-mail bezorgen: poort 25 etc. Een verbinding tussen twee systemen is uniek geïdentificeerd door het IP-adres en poortnummer van de ene en de andere kant van de verbinding.

Uitgaande sessies (dus geïnitieerd vanaf een werkstation op uw lokale netwerk) vinden normaliter alleen plaats vanaf een poort hoger dan 1023 (dit zijn de 'hoge poorten'), de meest belangrijke applicaties gebruiken 'lage poorten' (1-1023). Voor werkstations, welke over het algemeen geen applicaties behoren aan te bieden, is het netwerk op de lage poorten afgeschermd. Hierdoor kan er vrijwel alleen verkeer inkomen dat geïnitieerd is vanuit uw eigen netwerk.

De tweede reeks staat in principe 'open' voor inkomend verkeer, zodat u diensten aan kennisnet en kennisnetgebruikers kunt aanbieden, of systemen bereikbaar kunt maken vanaf kennisnet. Zo kunt u in deze reeks uw eigen webserver of mailserver plaatsen.

De derde reeks is volledig afgeschermd. Er komt geen bit aan data doorheen.

Naast deze maatregelen voor specifieke delen geldt voor de gehele adresreeks een aantal maatregelen.

- **NetBIOS dicht**. NetBIOS is het protocol dat met name door Windows-systemen onderling wordt gebruikt om bestanden uit te wisselen en afdrukopdrachten naar printers te sturen. Dit protocol en de implementatie ervan is in het verleden gebleken niet 100% waterdicht te zijn en gevoelig voor inbraak. Het is daardoor een risico om het open te stellen voor geheel kennisnet.
- **Standaard cracking-poorten**. De standaardpoorten van een aantal bekende 'cracking-tools', zoals BackOrifice en NetBus, zijn dichtgemaakt. Dit soort software komt meestal als een soort 'Trojaans Paard' binnen. Hiermee bent u **uitsluitend** beveiligd tegen aanvallen van buitenaf via de standaardpoorten. Vaak kunnen de 'tools' ook op afwijkende poorten luisteren.
- **Beveiliging tegen 'broadcast'**. Een 'broadcast' is een signaal naar een speciaal IP-adres in uw IP-reeks, het broadcastadres. Bij een bericht naar dit adres zouden theoretisch **alle** computersystemen op uw netwerk kunnen reageren. Er is een aanval bekend, de zogenoemde Smurf-aanval, waarbij uw netwerk als een soort versterker zou fungeren. Er wordt in dat geval een reeks pakketjes naar uw netwerk gestuurd met een vervalst afzenderadres. De systemen op uw netwerk die op het broadcastadres reageren, sturen dan massaal een antwoord naar het valse afzenderadres, waardoor uw netwerkverbinding en de ontvanger van de antwoorden het ‘erg druk’ krijgen. Dit is binnen kennisnet afgeschermd.

2.3 Is mijn netwerk 100% veilig op kennisnet?

Helaas, nee, 100% veiligheid is niet mogelijk. Er zijn namelijk nogal wat gevaren die op de loer liggen, waartegen door kennisnet maar moeilijk iets te doen is.

- **Virussen**. De bestrijding van virussen loopt eigenlijk altijd achter de feiten aan. Voordat er een 'vaccin' kan worden gemaakt door de producenten van antivirussoftware, moet het virus eerst een tijd actief zijn. Virussen die zich – zoals 'Melissa' en 'I Love You' – via e-mail verspreiden, gaan vaak erg snel. De beste remedie daartegen is zorgen dat verdachte aanhangsels van e-mail niet worden geopend. Ook software die u van het Internet ophaalt, kan verdacht zijn: accepteer alleen software van vertrouwde web- en FTP-sites. **Instrueer uw gebruikers om hier verstandig mee om te gaan.**
- **Lekken in software**. Software is zelden foutvrij. Foutvrije software van enige omvang bestaat al helemaal niet. Met de regelmaat van de klok worden fouten ontdekt in software, die kleine of grote gevolgen kunnen hebben voor de beveiliging van computersystemen. Het gaat vaak om exotische situaties die zelden voorkomen, maar áls ze dan voorkomen, kunnen soms speciale instructies worden uitgevoerd en gehele of gedeeltelijke controle over het betreffende systeem worden verkregen. Als er bijvoorbeeld een 'lek' in uw webserver zit en iemand weet daar vanaf kennisnet of zelfs vanaf het Internet gebruik van te maken, dan kan dat de veiligheid van uw webservice tenietdoen. Houd daarom uw software actueel en breng alle door de leverancier aangeraden beveiligingen aan. Activeer **nooit** meer services dan absoluut noodzakelijk (of schakel uit wat u kunt missen).

- **Kwaadwillende eigen gebruikers**. De personen die er het meeste belang bij hebben dat uw systemen worden gecompromitteerd, zouden wel eens uw eigen gebruikers kunnen zijn! Veel aanvallen op computersystemen vinden plaats van binnenuit. Dit is iets om ernstig rekening mee te houden. Het is bijvoorbeeld aan te raden om uw administratieve netwerk te scheiden (fysiek of via een eigen firewall) van het leerlingennetwerk en de kennisnetkoppeling. Van zaken die zich op het administratienetwerk bevinden, maar ook op het leerlingennetwerk beschikbaar moeten zijn, zou u een kopie kunnen maken op een separaat systeem.
- **'Verloren' wachtwoorden**. Een veelvoorkomend probleem is dat wachtwoorden worden gekraakt of achterhaald. Dit kan gebeuren indien uw wachtwoord te eenvoudig is of bij teveel mensen bekend is. Als u een wachtwoord met veel mensen deelt, kan het een eigen leven gaan leiden. Schrijf uw wachtwoord bij voorkeur **niet** op, maar probeer een wachtwoord te vinden, dat u eenvoudig kunt onthouden, maar dat niet eenvoudig te raden is voor anderen.
- **Cracking tools**. Eigenlijk hoort dit ook onder de virussen, omdat veel cracking-tools, zoals BackOrifice en NetBus, als Trojaanse Paarden binnenkomen. In de beveiligingsfilters in de routers zijn weliswaar maatregelen genomen tegen onder andere BackOrifice en Netbus, maar alleen op de standaardpoorten. Het is onmogelijk om het netwerk op alle mogelijke poorten te sluiten, want dat zou betekenen dat uw complete netwerk wordt gesloten. Ook komen er steeds nieuwe 'tools' bij die weer andere poortnummers gebruiken. Het duurt dus enige tijd voordat alles weer kan worden bijgesteld. Ook hier geldt: voorkomen is beter dan genezen; probeer waar mogelijk te voorkomen dat uw systemen dergelijke 'virussen' oplopen.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen aan 'handboek@kennisnet.nl'.

Index

Figurenlijst

Datum : 15 juni 2000
Versie : 20000615.01
Documentnr.: 995047

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel VII, Veelvoorkomende vragen

Indeling van dit document

Dit deel van Het Handboek behandelt een aantal veelvoorkomende vragen rond kennisnet en de diensten die door kennisnet worden aangeboden.

In Hoofdstuk 1 worden vraagstukken rond e-mail behandeld.

Hoofdstuk 2 gaat in op vragen rond 'surfen' op het wereldwijde web.

In Hoofdstuk 3 wordt ingegaan op vragen rond het correct gebruik van het Internet en kennisnet, waaronder de 'Netiquette'.

Hoofdstuk 4 behandelt een aantal problemen die kunnen voorkomen en hoe u deze problemen kunt analyseren.

Hoofdstuk 5 gaat in op een aantal vragen rond aanvullende dienstverlening en uitbreiding/aanpassing van de dienstverlening van kennisnet.

Inhoudsopgave

Hoofdstuk 1. E-mail

1.1 Waar haal ik de e-mailadressen vandaan?

Na of mogelijk al vóór de aansluiting van uw school of instelling ontvangt de ICT-coördinator per post een brief met daarin de gegevens (gebruikersnaam, wachtwoord, postbusnummer / e-mailadres) voor de ICT-coördinator. In de postbus vindt u een e-mailbericht met alle gegevens van de andere gebruikers van uw school of instelling: medewerkers, docenten, studenten of leerlingen. Indien u hiermee niet uit de voeten kunt, kunt u de lijst ook op diskette aanvragen.

1.2 Hoe kunnen de e-mailadressen en gebruikersnamen aan personen worden gekoppeld?

In Deel IV ‘Diensten’ wordt alles rond het beheren van gebruikers binnen uw organisatie uitgelegd. Hieronder valt het koppelen van gebruikersnamen en e-mailadressen aan personen. Ook wordt uitgelegd hoe u wachtwoorden kunt wijzigen.

1.3 Wat is POP(3) en wat is IMAP(4)? Wat is het verschil?

POP3 is de derde en meest actuele versie van het 'Post Office Protocol'. IMAP4 is de vierde en meest actuele versie van het 'Internet Mail Access Protocol'. Beide zijn protocollen om e-mail op te halen en te lezen. Het grote verschil zit feitelijk in het doel waarvoor het protocol het beste gebruikt kan worden.

POP3 is voornamelijk bedoeld om post op te halen naar de lokale computer, daar op te slaan en vervolgens van de server te verwijderen. Alle verdere bewerkingen dienen op de lokale machine plaats te vinden. Om post in mappen op te slaan, dienen in het lokale e-mailprogramma mappen gemaakt te worden.

IMAP4 is vooral bedoeld in gevallen waarin het handig is om de berichten op de server achter te laten. IMAP4 voorziet in mogelijkheden om de berichten op de server al in verschillende mappen in te delen. IMAP4 kent zowel mappen op de server als lokale mappen (op de eigen computer), waartussen u de berichten heen en weer kunt slepen. Hierdoor kunt u, afhankelijk van bijvoorbeeld de beschikbare schijfruimte, bepalen waar u uw berichten wilt opslaan.

POP3 biedt ook de mogelijkheid om de berichten (tijdelijk) op de server achter te laten (Engels: 'leave on server'), maar u kunt niet zoals bij IMAP4 de berichten tussen lokale mappen en mappen op de server heen en weer slepen

Wat het beste protocol is in uw situatie, zult u zelf moeten beslissen.

1.4 Wat is 'SPAM'?

SPAM is ongewenste en/of ongevraagde e-mail, in het Engels 'unsollicited mail'. Het betreft vaak berichten die uitnodigen om websites te bezoeken. Nogal eens gaat het om zogenaamde 'adult'-sites, aanbiedingen om veel geld te verdienen met kettingbrieven, reclame voor van alles en nog wat, etc. Soms zijn het vrij onschuldige kettingbrieven, vaak ook kettingbrieven die zogenaamd geluk brengen, maar volgens de tekst ongelukken veroorzaken als de brief niet op tijd wordt doorgestuurd. Allemaal onzin.

'SPAM' is ook een Amerikaans merk van blikken vlees; hierover worden wel eens grappen gemaakt: zie ook http://www.spam.com/ [1].



1.5 Wat moet ik met SPAM doen?

Niets. U kunt deze berichten het best negeren en weggooien. Soms is het zinvol om de beheerder van het domein waar het bericht vandaan komt, in te lichten, zodat deze maatregelen kan nemen. Het vereist echter gedegen kennis van e-mail om de werkelijke zender te achterhalen.

1.6 Wat kan ik tegen SPAM doen?

Sommige e-mailprogramma's bieden de mogelijkheid om een lijst met ongewenste e-mailadressen aan te leggen. Dit biedt echter geen 100% oplossing, omdat veel 'spammers' niet-bestaande e-mailadressen gebruiken. De e-mailvoorzieningen van kennisnet bieden echter al bepaalde voorzieningen. De belangrijkste maatregel is dat het mailsysteem weigert de berichten van niet-bestaande domeinnamen te accepteren.

1.7 Wat is SPAM-relay?

Veel 'spammers' proberen hun berichten te bezorgen via machines van andere organisaties om zo te proberen hun eigen identiteit te verhullen en het te laten lijken of het bericht van zo'n andere organisatie afkomstig is. Zo voorkomen de spammers dat alle boze berichten bij hen terugkomen.

SPAM-relay is dus het doorsluizen van SPAM-berichten via machines van andere organisaties.

1.8 Welke maatregelen kunnen worden getroffen tegen SPAM-relay?

Veel serversoftware voor e-mail – waaronder ook de software van Netscape, die in het serverpark van kennisnet wordt gebruikt, en Sendmail, het meest gebruikte mailpakket – biedt al mogelijkheden om SPAM-relay tegen te gaan. De truc is dat voor elke inkomende verbinding wordt bekeken van welk IP-adres de verbinding afkomstig is. Als het een lokaal IP-adres betreft of in ieder geval een IP-adres dat door de server wordt herkend als 'van de eigen organisatie', mag de zender in principe naar elk adres zenden. Vanaf alle andere IP-adressen mag alleen e-mail worden bezorgd voor de 'eigen organisatie' van de server.

Een andere oplossing is 'authenticated SMTP', een uitbreiding op het protocol dat voor verzending van e-mail wordt gebruikt. Hierbij dient de gebruiker zijn identiteit (door middel van een gebruikersnaam en wachtwoord) kenbaar te maken. Pas als dit blijkt te kloppen, kan de gebruiker zijn berichten verzenden. Deze optie wordt echter *niet* ondersteund door de mailservers van kennisnet.

1.9 Wat is een signature?

Een 'signature' is een kenmerk van een gebruiker, dat deze onder zijn/haar e-mail- en nieuwsberichten kan plaatsen. Meestal vermeld de 'signature' de naam en enkele adresgegevens (e-mail, webpagina etc.) van de afzender van het bericht, maar sommige personen zijn zo creatief dat er met wat karakters hele kunstwerken worden gemaakt.

[1] Bron afbeelding: http://www.spam.com/.

Er zijn ook diverse websites waar verzamelingen van 'signatures' worden bijgehouden. Een aantal voorbeelden in Nederland:

- http://huizen.dds.nl/~mwpieter/sigs[2]
- http://grid.let.rug.nl/~welling/sigs.html
- http://home.wxs.nl/~faase009/Signindex.html
- http://www.sci.kun.nl/thalia/funpage/koej/ascii-koej.html
- http://www.lstock.demon.nl/sigs.html

De term 'signature' wordt ook gebruikt voor een zogenoemde controlesom die over een e-mailbericht kan worden berekend. Deze som wordt op een zodanige manier berekend, aangevuld met een geheime code, dat door middel van een publieke code gecontroleerd kan worden of het bericht *echt* van een bepaalde persoon afkomstig is. Het bekendste product dat dit doet, is PGP, voluit 'Pretty Good Privacy' ('redelijk goede privacy').

1.10 Ik krijg een waarschuwing dat ik een e-mailbericht met een bepaalde titel niet moet openen. Wat is er aan de hand?

Het lijkt wel of die berichten niet uit te roeien zijn. Dit soort berichten is vaak pure onzin. Er wordt vaak verteld dat het openen van een bepaald e-mailbericht, bijvoorbeeld 'Penpal greetings', ervoor kan zorgen dat uw gehele harde schijf wordt gewist. Dat kan **niet**. Een e-mailtje kan uw harde schijf niet wissen. Dit soort berichten wordt ook wel 'hoaxes' genoemd. Meer voorbeelden zijn te vinden op het adres http://ciac.llnl.gov/ciac/CIACHoaxes.html.

Let echter wel op met aanhangsels ('attachments') van e-mail. Hierin kunnen wél programma's of scripts worden verpakt, die bijvoorbeeld een virus of 'Trojaans Paard' kunnen bevatten. Scan dergelijke programma's altijd op virussen vóór ze te openen! Let vooral op het type bestand. De recente opschudding door virussen als ‘Melissa’ en ‘I Love You’ heeft wel geleerd dat u ook bestanden die u van vrienden, kennissen en collegae ontvangt, niet altijd kunt vertrouwen: ze kunnen immers buiten hun weten om illegaal zijn verstuurd!

1.11 Kan ik mijn e-mail buiten kennisnet ophalen?

Ja, door gebruik te maken van dezelfde servernamen (‘pop.kennisnet.nl’ en ‘imap.kennisnet.nl’), zowel binnen als buiten het kennisnet, kunt u uw e-mail ophalen. Dit geldt echter (nog) niet indien u een eigen mailserver hebt.

1.12 Kan ik mijn e-mail buiten kennisnet verzenden?

Nee, in principe niet, althans niet via kennisnet. U kunt de mailservers van kennisnet alleen binnen kennisnet gebruiken om e-mail te verzenden. Om bijvoorbeeld vanaf uw huisadres e-mail te verzenden, dient u de mailserver van uw lokale Internetaanbieder te gebruiken. U kunt als afzenderadres wel uw kennisnetadres gebruiken.

[2] Deze verzameling is door medeauteur Menno Pieters aangelegd.

1.13 Als ik e-mail van buiten kennisnet probeer te verzenden, krijg ik een foutmelding



Figuur 1: foutmelding

Indien u in Outlook de melding 'De SMTP-server heeft gereageerd met een fout. (Account: 'KennisNet', SMTP-server: 'smtp.kennisnet.nl', foutnummer: 0x800ccc60).' krijgt, dan betekent dit dat u geen e-mail via deze server kunt verzenden. Dit komt doordat er een beveiliging is ingesteld tegen 'SPAM-relay', het doorsluizen van ongewenste e-mailberichten naar externe adressen. Alleen computers binnen kennisnet mogen e-mail naar buiten kennisnet versturen via deze machine. Ook mag van buiten kennisnet alleen e-mail met een bestemming binnen kennisnet via deze machine worden verstuurd.

Netscape Communicator zal mogelijk vragen om een wachtwoord. Dit zal echter niet werken, omdat de mailserver niet met 'authenticated SMTP' (zie paragraaf 1.8) werkt.

Om e-mail te versturen buiten kennisnet, dient u gebruik te maken van de voorzieningen van uw lokale Internetaanbieder.

1.14 Kan ik mijn externe e-mail binnen kennisnet ophalen?

Nee, dit is niet mogelijk met POP of IMAP. Indien dat handig voor u is, zou u, indien uw aanbieder dit mogelijk maakt, uw e-mail kunnen laten doorsturen naar uw kennisnetadres. Een andere optie is om gebruik te maken van een speciale webmailsite, zoals http://www.twigger.nl/, http://www.webmail.nl/ of http://www.xoip.nl/, of via een eventuele eigen webmailserver van uw provider. Hier kunt u, met de juiste gegevens, uw e-mail ophalen, lezen en beantwoorden.

Hoofdstuk 2. Surfen

2.1 Wat zijn 'cookies'?

'Cookies' zijn kleine stukjes informatie die een website naar uw bladerprogramma kan sturen. Deze informatie kan gebruikt worden om bijvoorbeeld een boodschappenlijstje op te slaan in een elektronische winkel, maar ook om u toegang te verlenen tot delen van de website.

2.2 Zijn cookies gevaarlijk?

Eigenlijk niet, hoewel met cookies wel kan worden vastgelegd hoe u door een website 'gewandeld' bent, wat voor bepaalde aanbieders interessant kan zijn. Als men dat via een formulier weer aan uw naam en adresgegevens weet te koppelen, zou men dat kunnen gebruiken om u gericht reclame te sturen.

Cookies op zich zijn niet gevaarlijk, ze kunnen geen virussen bevatten en met cookies kan men geen andere gegevens over u opvragen dan door uzelf worden ingegeven. Toch kan het geen kwaad om 'Cookies' uit te zetten in uw bladerprogramma of om uw bladerprogramma te laten waarschuwen voordat een cookie wordt geaccepteerd. Sommige websites vereisen echter het gebruik van cookies om bepaalde informatie te benaderen; in dat geval kan het tijdelijk worden ingeschakeld.

2.3 Wat is Java?

Java is een programmeertaal om, vooral voor gebruik op het Internet, programma's te ontwikkelen. ‘Java-applets' zijn kleine programmaatjes die in een webpagina gebruikt kunnen worden om bepaalde functies te vervullen, zoals een plaatje laten bewegen, kleine spelletjes of een rekenmachientje. Java is zo ontworpen, dat het niet uitmaakt op welk type computer en welk besturingssysteem het wordt gebruikt.

2.4 Wat is JavaScript?

JavaScript is, net als Java, een programmeertaal. In Java kunnen echter complete programma's worden gemaakt en met JavaScript alleen extra functionaliteiten aan webpagina's toegevoegd worden. Vaak wordt JavaScript gebruikt om dynamische delen van een pagina te genereren, kleine berekeningen te doen of om formulieren te controleren vóór verzending.

2.5 Wat is ActiveX?

ActiveX is het antwoord van Microsoft op Java. Het is net als Java bedoeld om kleine stukjes programmatuur te bieden, die extra functionaliteit aan webpagina's toevoegen. Een belangrijk verschil is echter dat alleen bladerprogramma's die onder Windows werken, met ActiveX-componenten overweg kunnen.

2.6 Wat zijn 'plug-ins'?

'Plug-ins' zijn hulpprogramma's die uw bladerprogramma in staat stellen om met specifieke gegevens om te gaan en u bijvoorbeeld filmpjes te laten bekijken, geluiden te laten beluisteren, speciale documenten te laten bekijken, etc. In tegenstelling tot een Java-applet kan een plug-in niet zonder meer op elktype computer of met elk besturingssysteem werken; voor ieder verschillend 'platform' is een aparte plug-in nodig.

2.7 Ik wil iets zoeken op het Internet. Waar kan ik dat doen?

Op het Internet zijn er diverse zoekmachines ('search engines') die u in staat stellen om op basis van wat trefwoorden documenten, afbeeldingen en geluiden te zoeken. Er zijn zowel zoekmachines die alleen in Nederland zoeken, als machines die wereldwijd zoeken. Een aantal bekende zoekmachines wordt hieronder opgesomd. Deze lijst is **niet** compleet!

Altavista	http://www.altavista.com	Documenten	Wereldwijd
Altavista Photo Finder	http://image.altavista.com	Afbeeldingen	Wereldwijd
DejaNews	http://www.dejanews.com	Nieuwsberichten	Wereldwijd
Excite	http://www.excite.com	Documenten	Wereldwijd
Google	http://www.google.com	Documenten	Wereldwijd
ILSE	http://www.ilse.nl	Documenten	Nederland
Lycos	http://www.lycos.com	Documenten	Wereldwijd
Lycos Pictures and Sounds	http://www.lycos.com/picturethis/	Afbeeldingen en geluiden	Wereldwijd
Track	http://www.track.nl	Documenten	Nederland
Yahoo*!*	http://www.yahoo.com	Documenten	Wereldwijd
Vinden	http://www.vinden.nl	Documenten	Wereldwijd
Vindex	http://www.vindex.nl	Documenten	Nederland
Zoek.NL	http://www.zoek.nl	Documenten	Nederland

Er zijn ook zogenaamde 'agents', die voor u verschillende zoekmachines kunnen raadplegen en met een meer afgewogen antwoord komen. Een voorbeeld is 'Copernic' (voor Windows), dat in een gratis versie en een uitgebreidere 'professionele' versie te krijgen is. Copernic kunt u ophalen vanaf de website http://www.copernic.com/.

2.8 Is het gebruik van Secure Sockets Layer (SSL) mogelijk?

SSL wordt vaak gebruikt voor on line bankieren en winkelen, en voor andere zaken waarbij een hoge mate van privacy gewenst is. De proxyservers van kennisnet ondersteunen SSL voor HTTP (HTTPS) op dezelfde manier als zij normaal webverkeer (HTTP) ondersteunen. Zie Deel III van Het Handboek voor de instellingen voor uw bladerprogramma.

Hoofdstuk 3. Gebruik van het Internet en kennisnet

3.1 Wat is 'Netiquette'?

'Netiquette' is, net als de 'etiquette', een verzameling van gedragsregels voor de omgang met andere personen. De 'Netiquette' beschrijft hoe gebruikers van het Internet met elkaar op een nette manier kunnen communiceren. Deze regels leggen uit 'hoe het hoort'. Zo wordt het bijvoorbeeld niet netjes geacht om een e-mailbericht of een nieuwsbericht geheel in hoofdletters te schrijven. Woorden die geheel in hoofdletters worden geschreven, worden opgevat als 'schreeuwen'.

Ook wordt het niet gewaardeerd om berichten met een ellenlange 'signature' af te sluiten. Een 'goede' signature zou niet meer dan zo'n vier regels lang moeten zijn.

Uiteraard wordt het ook niet gewaardeerd wanneer men onheus bejegend wordt of voor ‘rotte vis’ wordt uitgemaakt. Eigenlijk zijn de 'regeltjes' over het algemeen redelijk vanzelfsprekend

Meer uitleg over de 'Netiquette' is te vinden op het onderstaande adres:

http://www.albion.com/netiquette/index.html.

3.2 Misbruik, klachten en reprimandes

Ondanks de 'Netiquette' komt het (helaas) nog wel eens voor dat gebruikers van het Internet zich, al dan niet met opzet, niet helemaal gedragen zoals het hoort. Er zijn zelfs organisaties die zich hieraan schuldig maken (georganiseerde 'spammers' bijvoorbeeld; zie ook paragraaf 1.4).

Het is uiteraard mogelijk om klachten in te dienen tegen afzenders van vervelende berichten. In het geval van de georganiseerde spammers heeft dit weinig of geen zin, maar tegen een individu zijn soms nog wel maatregelen mogelijk. Klachten over e-mailberichten kunnen meestal aan 'postmaster@*domein*' of 'abuse@*domein*' worden gestuurd. Klachten over de inhoud van een website kunnen meestal naar 'webmaster@*domein*' worden gestuurd. (Hierbij dient u @domein te vervangen door de betreffende domeinnaam.)

Het vergt enige moeite en kennis van zaken om met een redelijke zekerheid te achterhalen waar een e-mailbericht werkelijk vandaan komt en dus de juiste personen in te lichten. Deze personen zullen de betreffende misbruiker veelal een waarschuwing geven of een 'hartig woordje' met deze persoon willen spreken. Bij aanhoudende klachten nemen de bevoegde personen 'gepaste maatregelen'. Dit houdt meestal in dat de gebruiker de toegang tot de systemen wordt ontzegd en geen gebruik meer kan maken van het Internet en diensten.

Hoofdstuk 4. Problemen

In dit hoofdstuk worden enkele veelvoorkomende problemen behandeld.

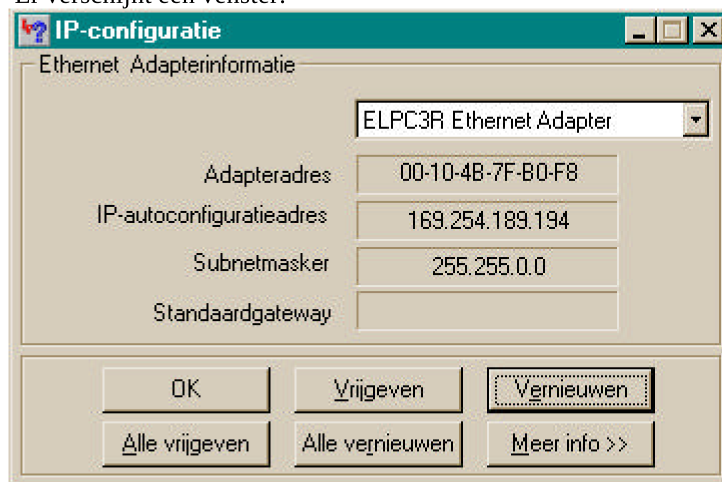
4.1 Ik krijg geen IP-adres. Wat moet ik doen?

Als u geen IP-adres krijgt van de DHCP-server, is het mogelijk dat de DHCP-server niet functioneert of niet bereikbaar is. Echter, voordat u het Servicepunt kennisnet gaat bellen, kunt u het best een aantal zaken controleren.

- Aangenomen dat u uw netwerk hebt aangesloten: controleer of op beide aansluitingen (op de hub en/of het kabelmodem en/of de router én op de computer) een lampje brandt. Dit is meestal een klein groen LED-je. Als dat niet het geval is, is mogelijk de bekabeling defect of is de verkeerde bekabeling gebruikt. Zie in Deel II van Het Handboek voor meer informatie.
- Controleer of op uw computer de juiste software en besturingssoftware is geïnstalleerd. Voor Windows 3.1/3.11 dient u mogelijk een extra pakket – bijvoorbeeld Trumpet WinSock – te installeren om gebruik te maken van TCP/IP. Onder Windows 95/98 ient ondersteuning voor TCP/IP geïnstalleerd en geconfigureerd te zijn (zie Deel III van Het Handboek). Op de Macintosh dient MacTCP en bij voorkeur ook OpenTransport geïnstalleerd en geconfigureerd te zijn (zie Deel III van Het Handboek).
- Probeer om 'met de hand' een IP-adres te krijgen.

  In Windows 95/98 kunt u dit doen met het programma WinIPCfg. Ga naar de startknop van Windows, selecteer 'Uitvoeren…'. Typ in het venster dat dan verschijnt, de opdracht '`winipcfg`' en klik op 'OK'.

  Er verschijnt een venster:



  Figuur 2: WinIPCfg

  Selecteer uw 'ethernetadapter', dus niet de PPP-adapter. Klik op 'Vrijgeven' en vervolgens op 'Vernieuwen'. Nu zou binnen enkele seconden een IP-adres moeten verschijnen. Indien u een adres krijgt dat begint met '`169.254`', dan is een fout opgetreden. Hier zou eigenlijk '`0.0.0.0`' moeten verschijnen, maar Microsoft heeft het '`169.254`'-netwerk gebruikt om zonder DHCP-server met computers onderling te kunnen communiceren.

- Onder Windows dient u gebruik te maken van een tekstuele applicatie, die u vanaf de commandoregel in een 'CMD'- of 'DOS'-venster[3] dient aan te roepen: `IPCONFIG`'. Wanneer de optie '`/?`' wordt meegegeven, worden de mogelijke opties getoond.

  Om een nieuw IP-adres te verkrijgen, dient u eerst het oude weg te gooien en dan opnieuw een adres aan te vragen. Hierbij dient u echter de aanduiding van de netwerkaansluiting te vermelden. Deze krijgt u te zien wanneer u het commando `IPCONFIG`' *zonder* parameters start. In het onderstaande voorbeeld is de aanduiding '`N1001`'.

  De te geven opdrachten voor het aanvragen van een nieuw IP-adres zijn dan:

  - Vrijgeven oud adres `IPCONFIG /RELEASE N1001`
  - Nieuw adres aanvragen `IPCONFIG /RENEW N1001`

  In Figuur 3 is een voorbeeld gegeven van hoe een nieuw IP-adres kan worden aangevraagd.

```
Command Prompt

C:\>ipconfig /?

Windows NT IP Configuration

usage: ipconfig [/? | /all | /release [adapter] | /renew [adapter]]

       /?       Display this help message.
       /all     Display full configuration information.
       /release Release the IP address for the specified adapter.
       /renew   Renew the IP address for the specified adapter.

The default is to display only the IP address, subnet mask and default gateway
for each adapter bound to TCP/IP.

For Release and Renew, if no adapter name is specified, then the IP address
leases for all adapters bound to TCP/IP will be released or renewed.

C:\>ipconfig /release N1001

Windows NT IP Configuration

IP address 10.17.42.12 successfully released for adapter "N1001"

C:\>ipconfig /renew N1001_
```

Figuur 3: IPCONFIG

- Op de Apple Macintosh kunt u dit doen door het regelpaneel 'TCP/IP' te openen, een andere configuratie actief te maken en terug te schakelen naar de configuratie die DHCP gebruikt. Een andere manier die veelal werkt, is om de Macintosh in 'sluimerstand' te zetten, via het menu of met de toetsencombinatie 'Command-Shift-0 [= nul]' en weer 'wakker' te maken met een willekeurige toetsaanslag.

Indien het ondanks alles niet lukt om een geldig IP-adres te krijgen, kunt u het beste het Servicepunt kennisnet bellen.

[3] Dit start u via de 'Start'-knop, 'Programma's' en dan 'CMD'.

4.2 Ik kan geen e-mail ophalen. Wat nu?

Controleer alle instellingen van uw e-mailprogramma, zoals gegeven in Deel III van Het Handboek. Indien het dan nog niet lukt, controleer dan of u een verbinding hebt met de mailservers. U kunt dit doen door met een speciaal programma[4] een 'ping' uit te voeren naar 'pop.kennisnet.nl' of 'imap.kennisnet.nl'. Controleer vervolgens of u de juiste gebruikersnaam en het juiste wachtwoord hebt ingevoerd. Als u dan nog uw mail niet kunt ophalen, schrijf dan nauwkeurig de foutmelding op en bel het Servicepunt kennisnet.

4.3 Ik kan de webserver van kennisnet niet bereiken

Allereerst dient u de TCP/IP-instellingen van uw besturingssysteem en bladerprogramma te controleren, zoals beschreven in Deel III van Het Handboek. Indien dat allemaal in orde is en u bovendien een geldig IP-adres krijgt, probeer dan of u de proxyservers kunt bereiken door – zoals in paragraaf 4.2 beschreven – een 'ping' uit te voeren naar 'proxy.kennisnet.nl'. Als deze functioneert, zou u naar het Internet moeten kunnen en daarmee naar http://www.kennisnet.nl/. Als dat niet lukt, kunt u een storing melden bij het Servicepunt kennisnet. Zorg dat u alle gegevens bij de hand hebt en zoveel mogelijk details van de storing kunt melden.

4.4 Als ik met Telnet of FTP mijn server probeer te bereiken, dan duurt het heel erg lang voordat deze reageert

U gebruikt waarschijnlijk een Unix-achtig systeem, zoals Solaris, FreeBSD of Linux. De serversoftware op deze systemen doet veelal een poging om de naam van de computer die probeert te verbinden, terug te vinden via de DNS-server. Zolang er nog private IP-adressen worden gebruikt, bestaat er binnen kennisnet nog geen DNS voor de computersystemen op de scholen. Hierdoor kan de DNS-server geen naam bij het betreffende IP-adres vinden en na een bepaalde tijd zal deze het zoeken opgeven en kunt u alsnog telnetten of FTP-en.

Een (tijdelijke) oplossing voor dit systeem is om op de server een bestand te plaatsen met de naam /etc/hosts, waarin u de IP-adressen en namen van de werkplekken dient op te nemen. Het bestand heeft de volgende opmaak: een IP-adres, een aantal spaties of een tab, een lange naam inclusief domein, wederom een aantal spaties of een tab en een korte naam zonder domeinnaam. Het verdient aanbeveling om een unieke naam voor iedere werkplek op te nemen, bijvoorbeeld uw BRIN- en vestigingsnummer en een nummer voor de werkplek. Hieronder volgt een voorbeeld.

```
10.1.2.1     99ZZ00-0001.kennisnet.nl   99ZZ00-0001
10.1.2.2     99ZZ00-0002.kennisnet.nl   99ZZ00-0002
10.1.2.3     99ZZ00-0003.kennisnet.nl   99ZZ00-0003
10.1.2.4     99ZZ00-0004.kennisnet.nl   99ZZ00-0004
10.1.2.5     99ZZ00-0005.kennisnet.nl   99ZZ00-0005
...
```

4.5 Ondersteunt Novell BorderManager meerdere C-klassen (blokken van 256 IP-adressen)?

Helaas, nee. Novell BorderManager kan uitsluitend met gehele C-klassen overweg. Novell heeft echter aangekondigd ‘supernetting’ (meerdere blokken van 256 IP-adressen) op korte termijn te zullen ondersteunen.

[4] Er zijn diverse gratis hulpmiddelen te krijgen, bijvoorbeeld 'NetLab' voor Windows, dat u via http://tucows.a2000.nl/ of http://www.tucows.com/ kunt vinden, of OTTool voor de Macintosh.

4.6 Ik kan het Internet niet bereiken!

Wat bedoelt u precies? Deze melding komt heel vaak binnen, maar of het een echte 'storing' is, ligt een beetje aan wat u precies wilt. U kunt namelijk voor geen enkele dienst *rechtstreeks* een verbinding maken naar systemen buiten het kennisnet. U dient gebruik te maken van een voor de gewenste dienst beschikbaar gestelde proxy (zie Deel III van Het Handboek). Indien die instellingen niet goed staan, kunt u het Internet inderdaad niet bereiken.

Indien u ervan overtuigd bent dat deze instellingen wél correct zijn, kan er sprake zijn van een storing. Schrijf de melding die u van uw programma krijgt, op en meld deze aan Servicepunt kennisnet.

Let op dat het mogelijk is dat u niet zonder meer met 'ping' kunt controleren of systemen buiten kennisnet bereikbaar zijn. In principe wordt al het verkeer tussen kennisnet en het Internet geblokkeerd, met enkele speciale uitzonderingen voor de servers van kennisnet zelf.

4.7 Kan ik mijn verbinding testen op snelheid?

Het **goed** testen van de snelheid van een verbinding is niet eenvoudig. Zeker over langere afstanden is het erg moeilijk om met zekerheid de snelheid van een verbinding te bepalen. Er zijn vele meetmethoden voor netwerkcapaciteit, netwerkvertraging etc. Helaas geven deze methoden vaak erg verschillende resultaten.

Vaak wordt geprobeerd om de netwerksnelheid te testen door 'even' een bestandje op te halen of te verzenden met FTP. Dit is vaak geen goede indicatie en wel om de volgende redenen:

- het ene FTP-programma is logger (en trager) dan het andere;
- de implementatie van TCP/IP in een besturingssysteem kan te wensen overlaten;
- de locatie waar het bestand vandaan komt, is ook een factor die het resultaat negatief kan beïnvloeden, want:
  - de server kan het erg druk hebben,
  - de verbinding van de betreffende server met het Internet kan traag zijn;
- de snelheidsindicatie van FTP-software is niet altijd eenduidig. Netwerksnelheden worden meestal uitgedrukt in kilobits of megabits per seconde (kb/s of Mb/s; let op de hoofd- en kleine letters). De snelheidsindicaties van FTP-software is soms wel in kilo**bytes** of mega**bytes** per seconde (kB/s of MB/s). Dat scheelt een factor acht! Doordat niet alle programma's correct hoofd- en kleine letters weergeven, kan het vaak lijken dat de snelheid te laag is.

Ongeveer dezelfde argumenten gelden voor HTTP. Daar komt echter nog bij dat informatie via HTTP vaak wordt gecodeerd op een dusdanige manier, dat ongeveer anderhalf keer zoveel data wordt verzonden als uiteindelijk op uw harde schijf belandt.

Indien u vermoedt dat uw verbinding te traag is, neem dan a.u.b. contact op met het Servicepunt kennisnet. Hier kan men opdracht geven aan personen met kennis van het netwerk en geschikte meetmethoden om een indicatieve meting uit te voeren. Indien daar aanleiding voor is, kan er een specifieke en meer nauwkeurige meting ter plaatse voor uw aansluiting worden uitgevoerd.

Overigens wordt er tijdens het aansluiten van uw school reeds een meting van de capaciteit uitgevoerd. Indien hieruit blijkt dat de aansluiting niet voldoende presteert, zullen maatregelen genomen worden.

4.8 Waarom is kennisnet op sommige momenten traag?

Over het algemeen is het netwerk van kennisnet zelf niet de remmende factor. Het netwerk biedt vooralsnog voldoende capaciteit. Deze wordt voortdurend gecontroleerd om te zorgen dat er op tijd extra capaciteit kan worden ingeschakeld.

Wel kunnen de proxyservers bij zeer zware belasting ietwat minder vlot reageren. Ook dit hoeft niet per se tot ernstige vertragingen te leiden. Een belangrijke factor bij de beantwoording van deze vraag is de plaats waar de machine waarmee u een verbinding probeert te maken, zich bevindt. Wanneer deze aan de andere kant van de oceaan (in Amerika) staat, zal het naarmate de dag vordert moeilijker worden om een vlotte verbinding met het systeem op te bouwen. Het dagelijks leven in Amerika komt zo'n zes tot tien uur later (afhankelijk van de tijdzone) op gang dan in Europa.

Verbindingen met het Verre Oosten (onder andere Japan, Taiwan) lopen vaak via Amerika en zijn daardoor soms ook tergend langzaam. Hier kan kennisnet helaas niet veel aan doen.

4.9 Waar kan ik een probleem melden?

Indien u problemen ondervindt bij het gebruik van kennisnet, kunt u contact opnemen met het Servicepunt kennisnet (zie Bijlage A). Mogelijk is men in staat u weer op weg te helpen met lokale problemen, of kan men u de weg wijzen in Het Handboek. Wanneer het problemen betreft met het landelijke of kabelnetwerk van kennisnet, of problemen met de diensten van kennisnet, kunt u via hetzelfde telefoonnummer uw problemen doorgeven, waarna de beheerorganisaties met de problemen aan de slag zullen gaan.

Zorg altijd dat u zoveel mogelijk informatie over de problemen beschikbaar hebt, zodat u zo goed mogelijk duidelijk kunt maken waar u exact problemen mee hebt. Dit komt de oplossing van het probleem zeer ten goede.

4.10 Waarom worden werkzaamheden niet aan scholen gemeld voordat ze plaatsvinden?

Het is gebruikelijk dat grote werkzaamheden minimaal een week voordat deze worden uitgevoerd, via de website van kennisnet (http://www.kennisnet.nl/) worden aangekondigd, zodat u er rekening mee kunt houden. Soms zal er via een e-maillijst een bericht worden verzonden naast de aankondiging op de website. Het is echter niet altijd mogelijk om elke school een persoonlijke brief en/of fax te sturen.

Hoofdstuk 5. Aanvullende diensten

5.1 Ik wil graag een (extra) aansluiting op kennisnet. Kan dat?

Neem a.u.b. contact op met het Servicepunt kennisnet: telefoon 0800-KENNISNET (0800-536647638). Daar kan men u precies vertellen hoe en waar u uw verzoek kunt indienen.

5.2 Hoe kan ik mijn aansluiting opzeggen?

Neem ook hiervoor a.u.b. contact op met het Servicepunt kennisnet, via 0800-KENNISNET (0800-536647638). Daar kan men u precies vertellen hoe en waar u uw verzoek kunt indienen.

5.3 Wat moet ik doen als onze school gaat verhuizen?

Daar komt heel wat bij kijken. Uw aansluiting zal moeten worden verplaatst. Mogelijk komt u in het verzorgingsgebied van een andere kabelmaatschappij. Bovendien is het waarschijnlijk dat uw IP-adressen zullen veranderen.

Het is, zoals gebruikelijk, wenselijk de verhuizing ruimschoots op tijd bij het Servicepunt kennisnet te melden. U ontvangt een formulier waarop u de wijzigingen kunt aangeven: nieuw adres of nieuwe adressen, ander aantal werkplekken, etc. Als uw school fuseert of een aantal vestigingen samengaat, is de operatie mogelijk nog wat ingrijpender.

5.4 Ik zou graag enkele wijzigingen in mijn aansluiting of de gebruikte diensten willen.

Ook dat kunt u allemaal via het Servicepunt kennisnet aanvragen. Er is een aantal formulieren beschikbaar, waarop u uw wensen kenbaar kunt maken. Er zal contact met u opgenomen worden om alle zaken door te nemen en te bekijken wat de mogelijkheden zijn.

Indien het een standaardondersteunde dienst betreft, kunt u binnen een vastgestelde periode een reactie en realisatie van uw wensen verwachten. Als u zeer speciale wensen hebt, zal het mogelijk wat langer duren.

5.5 Waar kan ik een aanvraag indienen om mijn IP-reeks te vergroten of te verkleinen?

U kunt een e-mailbericht sturen aan `servicedesk@nltree.nl` of bellen met het Servicepunt kennisnet: telefoon 0800-KENNISNET (0800-536647638), optie 3. Hier kan men u helpen; eventueel wordt verzocht om de benodigde informatie om het verzoek te kunnen verwerken.

5.6 Waar kan ik aanvragen voor het openstellen van routerpoorten indienen en wat zijn de stappen die hierop genomen gaan worden?

Bij veel van dergelijke verzoeken blijkt dat het helemaal niet nodig is om iets te doen en kan met het bestaande beveiligingsfilter worden gewerkt. Controleer in Deel I van Het Handboek of het echt nodig is om een dergelijk verzoek in te dienen. Poorten 1024 en hoger staan bijna allemaal open voor werkstations. Voor een deel van uw IP-reeks staan bijna alle poorten (behalve zeer kwetsbare poorten) open om diensten aan te bieden.

Indien het toch noodzakelijk blijkt om een wijziging in de instellingen van uw router uit te voeren, kunt u per fax een verzoek zenden aan nl.tree via faxnummer (070) 89 000 99. Het verzoek zal door het Ministerie van Onderwijs, Cultuur en Wetenschappen worden beoordeeld. Men neemt hiervoor contact op met uw instelling en zal een contract opstellen. Wanneer het contract ondertekend is geretourneerd, zal de technische realisatie in gang worden gezet.

5.7 Kan ik meer e-mailadressen/postbussen krijgen?

Indien u een tekort aan postbussen dreigt te krijgen, bijvoorbeeld doordat uw school qua leerlingenaantal snel groeit, kunt u extra postbussen laten aanmaken. Hiertoe kunt u een aanvraag indienen bij het Servicepunt kennisnet. Geeft u hierbij alstublieft aan waarom u extra postbussen nodig hebt en hoeveel u er wilt laten bijmaken.

5.8 Hoe kan ik een eigen domeinnaam aanvragen?

Het Servicepunt kennisnet heeft een formulier beschikbaar voor het aanvragen van domeinnamen voor e-mail en/of voor webservices. Via het Servicepunt wordt een verzoek ingediend bij de Stichting Internet Domeinregistratie Nederland (IDNL). Er wordt een procedure in gang gezet om te controleren of de door u gewenste domeinnaam niet strijdig is met de reglementen en of is voldaan aan bepaalde voorwaarden. Indien alles in orde is bevonden, wordt het domein, tegen betaling, aan u toegewezen. Vervolgens zal kennisnet de diensten verlenen om uw domein in werking te stellen, zoals DNS en dergelijke.

Meer informatie over dit onderwerp kunt u vinden op de website van de Stichting Internet Domeinregistratie Nederland: `http://www.domain-registry.nl/`. Hier vindt u onder andere het reglement, waarin wordt vermeld aan welke eisen een domeinnaam moet voldoen en wat niet mag. Er is ook een uitputtende lijst beschikbaar van domeinnamen die reeds geweigerd of gereserveerd zijn.

Let er wel op dat de aanvraag van een domeinnaam kosten met zich meebrengt: eenmalig voor de aanvraag en jaarlijks voor het behoud ervan.

5.9 Onze school heeft al een eigen domeinnaam. Kan deze door kennisnet worden overgenomen?

Dat is mogelijk. U dient een verzoek in te dienen bij het Servicepunt kennisnet met alle gegevens over de domeinnaam. Dit kan echter alleen indien *u* de eigenaar bent van de domeinnaam en niet uw provider. Bovendien, ook als *u* de eigenaar bent van de domeinnaam, is medewerking van uw huidige provider vereist.

Het verdient aanbeveling, indien u uw domein gebruikt voor meer dan één webserver en een bestemming voor uw mail, om een uitdraai van de 'zone-informatie' met uw verzoek mee te sturen.

5.10 Is het mogelijk om een Virtual Private Network (VPN) op te zetten binnen kennisnet?

Ja, dat is mogelijk. Op dit moment werkt kennisnet aan een standaardoplossing voor veilige verbindingen tussen schoollocaties. Deze oplossing wordt thans uitgeprobeerd tussen een aantal schoollocaties. Behalve de standaardoplossing zou u ervoor kunnen kiezen om een eigen VPN-oplossing te realiseren.

U dient er wel rekening mee te houden dat u mogelijk een snellere verbinding moet aanvragen om de vereiste capaciteit te kunnen garanderen. Veel verbindingen binnen kennisnet zijn bovendien asymmetrisch. Dat wil zeggen, dat de capaciteit van kennisnet naar uw instelling hoger is dan die van de weg terug. In het geval van een VPN zult u waarschijnlijk het heen- en terugwegverkeer gelijk willen hebben.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen aan 'handboek@kennisnet.nl'.

Index

Figurenlijst

Handboek
Aansluiting van het schoolnetwerk op kennisnet
Deel VIII, Begrippenlijst

Inhoudsopgave

Begrippenlijst

Dit hoofdstuk omvat een lijst met begrippen die met het Internet en kennisnet te maken hebben. Bij elk van deze begrippen volgt een korte uitleg.

Apple	Een fabrikant van computersystemen. Zie ook Macintosh.
Bastion Host	Een bastion host is een speciale router en/of gateway die ervoor zorgt dat ongewenst netwerkverkeer niet van of naar het eigen netwerk kan. Hiermee kan (tot op zekere hoogte) worden voorkomen dat er oneigenlijk gebruik wordt gemaakt van machines binnen het eigen netwerk door gebruikers van buiten het eigen netwerk. Vaak wordt een bastion host aangeduid als een 'firewall'.
BOOTP	BOOTP staat voor Bootstrap Protocol. De primaire toepassing van dit protocol was om een – vaak diskloos – werkstation van de juiste software en/of gegevens te voorzien om op te starten en in het netwerk mee te laten functioneren. BOOTP wordt, met de opkomst van opvolger DHCP, niet erg veel meer als specifieke dienst gebruikt. kennisnet ondersteunt dit ook niet, maar indien noodzakelijk is het mogelijk om een eigen systeem op te zetten.
DHCP	Dynamic Host Configuration Protocol. Dit protocol maakt het mogelijk om alle adresgegevens die een computer nodig heeft om verbinding te maken met kennisnet, centraal uit te delen.
Discussiegroepen	Zie 'News'
DMZ	DeMilitarized Zone. Zie ‘Gedemilitariseerde zone’
DNS	Domain Name Service. Dit kan het beste worden vergeleken met een soort telefoonboek of adressengids. Een DNS-server is in staat om een koppeling te maken tussen een machinenaam (bijvoorbeeld ‘www.kennisnet.nl’) en een IP-adres (bijvoorbeeld ‘195.61.115.2’).
E-mail	E-mail is een afkorting van 'electronic mail' ofwel elektronische post. E-mail is te vergelijken met een brief of faxbericht. E-mail is één van de belangrijkste toepassingen van het Internet, zo niet dé belangrijkste.
Ethernet	Een standaard waarmee computers op een lokaal netwerk kunnen communiceren. Boven op Ethernet kan bijvoorbeeld IP worden gebruikt om de machines onderling te adresseren.
Firewall	Een firewall is een verzameling van systemen die zorgen dat een intern netwerk wordt beveiligd tegen gevaren vanuit de buitenwereld. Tot een firewall worden gerekend: • een bastion host; • proxyservers; • een gedemilitariseerde zone (DMZ). Vaak wordt het woord 'firewall' gebruikt om een bastion host aan te duiden. Soms is dit inderdaad het enige onderdeel van de beveiliging.
FTP	File Transfer Protocol. Met dit protocol kunnen bestanden worden uitgewisseld tussen computers. Het protocol voorziet ook in een vertaaloptie van ASCII-tekstformaten tussen verschillende computerplatformen.
Gateway	Een gateway is een onderdeel van een netwerk dat toegang biedt tot een ander netwerk. Een gateway vertaalt veelal de verzonden informatie en adressen, zodat het andere netwerk deze ook begrijpt.

Gedemilitariseerde zone	Een gedemilitariseerde zone (ook: DMZ) is een deel van het netwerk, dat systemen omvat die rechtstreeks kunnen communiceren met de buitenwereld. Deze systemen vormen vaak een tussenstap voor de communicatie tussen het interne netwerk en de buitenwereld.
HTTP	HyperText Transfer Protocol, het protocol waarmee webpagina's op het wereldwijde web worden verzonden van de aanbieder naar de lokale computer. Zie ook ‘WWW’.
IMAP4	Interactive Mail Access Protocol, versie 4. Via dit protocol kan een e-mailprogramma berichten ophalen en terugplaatsen in een centrale e-mailopslag. Het protocol biedt goede mogelijkheden om e-mail centraal op te slaan en op een willekeurige plaats opnieuw te raadplegen.
Internet	Het Internet is een groot netwerk dat op zich weer onderverdeeld is in kleinere netwerken die onderling gekoppeld zijn. Het Internet is ooit ontstaan als een Amerikaans defensienetwerk (ARPANET). Later zijn ook educatieve en overheidsinstellingen aangesloten, en vervolgens andere netwerken in tientallen andere landen.
Intranet	Een intranet is een gesloten lokaal of bedrijfsnetwerk dat is gebaseerd op dezelfde technologie als die van het Internet.
IP	Internet Protocol. Dit protocol zorgt ervoor dat gegevens over een netwerk van de ene machine naar de andere machine getransporteerd kunnen worden op basis van een afzender- en een ontvangeradres. Boven op IP worden onder andere de protocollen TCP en UDP gedragen, die voor het transport en virtuele verbindingen zorg dragen.
IRC	Internet Relay Chat. IRC is een manier om met vele mensen tegelijk te kunnen 'chatten' (babbelen). Alle communicatie wordt via een centrale server geleid.
kennisnet	kennisnet is een landelijk, educatief computernetwerk, bedoeld om onder andere alle basis- en middelbare scholen alsmede instellingen voor agrarisch onderwijs en beroeps- en volwasseneneducatie met elkaar te verbinden.
LDAP	Lightweight Directory Access Protocol. Dit is een protocol om een soort adresboek ('directory') te raadplegen en te bewerken. In deze 'directory' bevinden zich de gegevens van alle gebruikers van kennisnet, waaronder hun gebruikersnamen, e-mailadressen en wachtwoorden.
Macintosh	Veelal afgekort als 'de Mac'. De Macintosh is een computersysteem van de fabrikant Apple. De Mac was de eerste, op grote schaal verkochte computer met een gebruikersvriendelijke grafische omgeving.
Masquerading	Een speciale vorm van NAT (zie ‘NAT’). Masquerading is ook wel bekend als n:1-NAT. In het geval van masquerading worden alle IP-adressen aan de binnenkant van het lokale netwerk vertaald naar één IP-adres aan de buitenkant van het lokale netwerk, en omgekeerd voor terugwegverkeer.
NAT	Network Address Translation. Dit is een techniek die het mogelijk maakt om IP-adressen op een lokaal netwerk zó te vertalen, dat deze bruikbaar zijn op het Internet en ook verkeer terug mogelijk is.
News	News, of ook 'Usenet News', is een systeem om middels een soort e-mailberichten met vele mensen tegelijk te kunnen discussieren over diverse onderwerpen. Er zijn op het Internet duizenden verschillende ‘discussiegroepen’. Daarnaast hebben sommige gesloten netwerken ook lokale discussiegroepen, zoals ook voor kennisnet het geval is.
NNTP	Network News Transfer Protocol. Dit is het protocol waarmee nieuwsberichten (zie 'News') worden uitgewisseld.

NTP	Network Time Protocol. Dit protocol wordt gebruikt voor een nauwkeurige tijdsynchronisatie. Dit protocol houdt onder andere rekening met de afstand tussen servers (lees: de tijd die een pakket nodig heeft om van de ene machine naar de andere te komen) en referentieservers. kennisnet biedt ook NTP om servers en werkstations te synchroniseren. Deze systemen zijn bereikbaar als '`time.kennisnet.nl`'.
POP3	PostOffice Protocol, versie 3. Dit protocol kan gebruikt worden om met een e-mailprogramma e-mail op te halen vanaf een mailserver. Het protocol is redelijk rechttoe rechtaan en biedt weinig extra mogelijkheden.
Proxy	De vertaling van het Engelse woord 'proxy ' is 'gevolmachtigde' of 'vertegenwoordiger'. Dit geeft ook redelijk aan wat een proxy doet: uit naam of op verzoek van de gebruiker haalt het gegevens op van, of legt het verbindingen met andere computers, veelal buiten het lokale netwerk van de gebruiker.
RFC	Een RFC (Request For Comment) is een document dat belangrijke informatie over Internetprotocollen, gebruiken of gedragsregels bevat. In RFC's worden standaarden en mogelijke aanstaande standaarden alsmede revisies hiervan beschreven. Voordat een protocol tot standaard wordt verheven, is er echter een lange weg afgelegd. De RFC-documenten kunt u o.a. vinden op het adres ftp://ftp.ripe.net/rfc/.
RJ45	Een specificatie voor een type aansluiting (stekkertje en contactje).
Router	Een router is een soort computer die zich uitsluitend bezighoudt met het in goede banen leiden van het netwerkverkeer. Als een pakketje aan de router wordt aangeboden met een bestemmingsadres, dan zal deze proberen het pakketje op een dusdanige manier door te sturen, dat het uiteindelijk op de juiste bestemming terecht zal komen.
RTSP	Real-Time Streaming Protocol. Dit is een protocol om beelden en geluiden in een ononderbroken stroom over het Internet te verzenden. Via dit protocol kunnen bijvoorbeeld radio-uitzendingen of tv-programma's via het Internet worden gevolgd, of korte filmpjes worden bekeken.
Serverpark	Het serverpark is een verzameling van grote computersystemen ('servers') die elk bepaalde diensten verzorgen voor kennisnet.
SMTP	Simple Mail Transfer Protocol. Dit protocol wordt gebruikt om e-mail op het Internet te verzenden van een e-mailprogramma naar een server, en tussen servers onderling.
SNTP	Simple Network Time Protocol. Dit protocol is een vereenvoudigde versie van NTP. SNTP biedt nog steeds een nauwkeurige manier om de tijd tussen twee systemen te synchroniseren, maar vereist iets minder zekerheden dan NTP. Zie 'NTP'.
TCP	Transmission Control Protocol. Dit protocol draagt zorg voor het opzetten van een (virtuele) verbinding tussen twee eindpunten en het, opgedeeld in pakketjes, verzenden van informatie. TCP garandeert dat de informatie aankomt en wel in de juiste volgorde. TCP vereist IP (het Internet Protocol) om te kunnen functioneren. IP zorgt voor de adressering, terwijl TCP voor een virtuele verbinding zorgt.

'Trojaans Paard' of 'Trojan Horse'	Een 'Trojaans Paard' is een programma dat, terwijl het wordt gebruikt, andere programmatuur op de computer probeert te besmetten met een computervirus. (De naam is afkomstig van de oude Griekse legende van de overwinning op de stad Troje, waarbij de aanvallende Grieken deden of zij zich gewonnen gaven en 'als geschenk' aan de stad Troje een houten paard achterlieten. In werkelijkheid zaten er soldaten in het houten paard, die 's nachts uit het door de Trojanen binnengehaalde paard klommen en de stad van binnenuit aanvielen.)
UDP	User Datagram Protocol. Dit protocol kan pakketjes informatie verzenden van één computer naar één of meer andere computers op een netwerk. In vergelijking met TCP heeft UDP minder mogelijkheden om fouten te herstellen en is de aankomst van de informatie niet gegarandeerd.
UNIX	UNIX is een merknaam van een besturingssysteem voor van origine grote computersystemen. Deze naam wordt echter ook gebruikt als verzamelnaam voor een complete familie van besturingssystemen die op hetzelfde idee zijn gebaseerd. Er zijn tegenwoordig ook uitvoeringen van dit besturingssysteem, die prima functioneren op gangbare computersystemen zoals PC's.
Virus	Een virus is een stukje programmatuur dat speciaal is gemaakt om zich te kopiëren en zichzelf verder te verspreiden. Veel virussen zijn bovendien zo geprogrammeerd, dat ze ook schade aanrichten onder bepaalde omstandigheden, na enige tijd op het systeem te hebben bestaan of op vaste tijdstippen (vrijdag de dertiende e.d.).
Web	Zie ‘WWW’.
Windows	Microsoft Windows is een grafische omgeving voor computers, waarmee men in staat wordt gesteld om speciale grafische programmatuur te gebruiken.
WWW	World Wide Web. Een systeem van wereldwijd verspreide informatie die op basis van ‘hyperlinks’ (verwijzingen) met elkaar is gekoppeld. Door de verwijzingen te selecteren, kunt u van de ene pagina met informatie naar de andere pagina surfen. De informatie kan bestaan uit opgemaakte teksten, afbeeldingen, beeld- en geluidsfragmenten.

Bijlage A. Belangrijke adressen en telefoonnummers

Scholen en andere aangesloten instellingen kunnen met vragen, opmerkingen en problemen terecht bij het Servicepunt kennisnet (SPK) van het Ministerie van Onderwijs, Cultuur en Wetenschappen. Het SPK is telefonisch te bereiken op het nummer 0800-KENNISNET (0800-536647638).

Voor op- of aanmerkingen, aanvullingen voor het 'Handboek kennisnet' kunt u e-mail sturen aan 'handboek@kennisnet.nl'.

Index